UNIVERSIDAD CARLOS III DE MADRID

TRABAJO FIN DE GRADO

ESTUDIO DE LA INTEROPERABILIDAD DE DISPOSITIVOS DE HUELLA DACTILAR – ANÁLISIS DE RENDIMIENTO DE DIFERENTES TECNOLOGÍAS.

GRADO EN INGENIERÍA ELECTRÓNICA INDUSTRIAL Y AUTOMÁTICA.

Autora: María Elvira Tomeo Martín
Tutora: María Belén Fernández Saavedra

Leganés, 25 de Septiembre de 2015

ÍNDICE DE CONTENIDOS

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

ÍNDICE DE ACRÓNIMOS

TFG	Trabajo Fin de Grado
UC3M	Universidad Carlos III de Madrid
GUTI	Grupo Universitario de Tecnologías de Identificación
ADN	Ácido Desoxirribonucleico
BBDD	Base de Datos
FTE	Failure to Enrol rate
FTA	Failure to Acquire rate
FNMR	False Non-Match Rate
FMR	False Match Rate
EER	Equal Error Rate
FRR	False Reject Rate
FAR	False Accept Rate
NBIS	NIST Biometric Image Software.
NIST	National Institute of Standards and Technology
FBI	Federal Bureau of Investigation
DHS	Department of Homeland Security
WPF	Windows Presentation Foundation

RESUMEN

Hoy en día, la tecnología supone una importante herramienta para todo tipo de personas, esto es debido a que ofrece comodidades, tanto a los usuarios más jóvenes como a los más adultos, en diferentes ámbitos de la vida diaria, como puede ser el trabajo, los estudios, el ocio o incluso la seguridad.

Uno de los campos que en las últimas décadas ha sufrido un progreso importante, gracias al avance de la tecnología, es el reconocimiento biométrico de personas mediante su huella dactilar. El adelanto más significativo conseguido en este terreno ha sido el abandono del método tradicional de recolección y comparación de las huellas dactilares en papel para dar paso a la utilización de un dispositivo electrónico, sensor de huella dactilar.

De este modo, son cada vez más las personas que utilizan como método de identificación en su vida diaria su huella dactilar, bien sea para realizar alguna acción bancaria, para mostrar su identidad en un aeropuerto, para acceder a una zona con acceso restringido o simplemente para desbloquear su ordenador, tablet o Smartphone.

Al igual que ocurre con los métodos de identificación tradicionales, la biometría necesita un proceso de recogida de datos, denominado reclutamiento, previo a cualquier identificación, para que cuando un usuario desee identificarse el sistema pueda comparar los datos introducidos en la identificación con los almacenados en el reclutamiento. Como se trata de identificación biométrica mediante huella dactilar el reclutamiento será el proceso por el cual se guarda la huella dactilar de un usuario en una base de datos para futuras identificaciones.

Con la introducción de los sensores de huella dactilar se introduce el problema de la interoperabilidad, dado que los sensores, las bases de datos y los algoritmos de reconocimiento no se encuentran estandarizados, lo que provoca errores cuando el reconocimiento de los usuarios se realiza con un sensor diferente al que se utilizó en el reclutamiento.

Debido a que la interoperabilidad es un problema actual, en el presente proyecto se ha realizado un estudio de análisis de interoperabilidad teniendo en cuenta sensores de diferentes tecnologías, para ello ha sido necesaria la creación de dos aplicaciones. La primera, implementada mediante la plataforma Visual Studio, necesaria para comparar, en diferentes pruebas, las huellas dactilares de una base de datos con el fin de evaluar, mediante la segunda aplicación, donde se incluye la herramienta "Biosecure Tool", como varía el rendimiento de dichos sensores al utilizar, en las identificaciones, un sensor diferente del utilizado en el reclutamiento.

Tras la realización del proyecto se ha comprobado que el rendimiento de los sensores de huella dactilar varía cuando se utiliza en las identificaciones un sensor diferente al que se utilizó en el reclutamiento, aumentando el rendimiento del conjunto si el sensor utilizado para las identificaciones proporciona imágenes de mejor calidad, y disminuyendo si se da el caso contrario, es decir, si el sensor de las identificaciones proporciona imágenes de peor calidad que el sensor de reclutamiento.

Palabras clave: biometría, huella dactilar, evaluación de rendimiento biométrico, sensores de huella dactilar, interoperabilidad entre sensores.

ABSTRACT

Nowadays, technology entails an important tool for everybody. This makes easier the daily live to young and elder people, especially in working and social tasks and even improving their security.

In the last decades, biometrics is one of the fields that has suffered an important development, thanks to the advances of fingerprint recognition technology. In particular, the most significant advance got in this area has been to leave the traditional methods to capture and compare fingerprints using ink and paper. Currently, fingerprints are obtained and compared automatically using electronic devices.

In this way, people uses their fingerprints to identify themselves in their daily life more often, for example to make any bank action, to access a restrict area or simply to unlock his computers, tablet or smartphones.

In a similar way to the classic identification methods, biometric needs a process to register the fingerprint in the system, called enrolment, before doing any identification. Then, when the user is going to conduct and identification, the system compares the fingerprint captures at that moment to the fingerprint registered during the enrolment.

The problem of the interoperability has been derived by the use of fingerprint sensors, as sensors and the recognition algorithms are not standardized. This fact causes errors when the recognition of the users is performance with a different sensor to the recruitment.

Due to the interoperability is an existing problem, this project have consisted on the analysis of the influence of fingerprints capture devices on biometric system performance. For doing it an application has been develop using the Visual Studio platform, to compare, the fingerprints of a data base collected using fingerprint scanners of different technologies. Specially two kind of experiments have been conducted: one in which similar fingerprints sensors are involved in the recognition process and other in which different sensors are used to execute such process. Then, using a tool for obtaining performance metrics, interoperability performance have been studied considering those trials.

After the project has been done, it can be said that biometric performance changes when different fingerprint scanners have been used for enrolment and recognition processes. This variation can be in two different ways. On the one hand, the biometric performance raises if the sensor used for the identification obtain images which quality is high. However the biometric performance decreases if the fingerprint sensors used for the identification capture images with a low quality.

Key words: biometrics, fingerprint recognition, performance testing of biometrics systems, fingerprint sensors, interoperability performance.

1. INTRODUCCIÓN

El presente documento describe el proyecto realizado como Trabajo de Fin de Grado (TFG). Dicho proyecto consiste en realizar un estudio de interoperabilidad de sensores de huella dactilar utilizados para el reconocimiento biométrico de las personas.

En ésta primera sección del documento se describen las motivaciones que han conducido a la autora a seleccionar este proyecto como etapa final del Grado en Ingeniería Electrónica Industrial y Automática. No obstante, se expondrán los objetivos de dicho proyecto, así como, el marco socio-económico y regulador donde se enmarca el mismo y una breve descripción de la estructura global del documento.

1.1 Motivación

En la primera mitad del último año del grado universitario de la alumna, se ofertó una beca para la realización de las prácticas de empresa en el Departamento de Tecnología Electrónica de la Universidad Carlos III de Madrid. Dichas prácticas estaban destinadas a la colaboración en un proyecto de investigación sobre el reconocimiento biométrico de personas mediante su huella dactilar, llevado a cabo por el Grupo Universitario de Tecnologías de Identificación, GUTI.

El proyecto consistía en la captura de datos biométricos a un gran volumen de usuarios, con el objetivo de recoger la mayor cantidad de huellas dactilares posibles, con los que poder realizar estudios y llegar a mejorar el rendimiento de los sensores de huella dactilar utilizados.

Durante este periodo se adquieren gran cantidad de conocimientos acerca de la biometría y el reconocimiento biométrico y se descubre un tema de elevado interés, lo que hace que surja en la alumna la necesidad de profundizar en él; necesidad que queda subsanada con la oferta del propio departamento de realizar uno de los proyectos de análisis nacidos tras la evaluación.

Uno de los principales puntos a estudiar en el reconocimiento biométrico es el rendimiento de los sensores utilizados para las capturas de huellas. Además, uno de los factores más influyentes actualmente en dicho rendimiento es la interoperabilidad de los sensores.

Por otro lado, la ilusión de este proyecto también viene dada por el vínculo que mantiene el problema de la interoperabilidad con la actualidad, ya que cada vez son más las acciones que se realizan diariamente utilizando como método de identificación personal la huella dactilar.

Como ejemplo de dicho problema podemos nombrar el reconocimiento biométrico de un usuario en una unidad bancaria. Cuando un usuario se registra por primera vez en la base de datos de un banco, lo va a realizar con el sensor de huella utilizado en dicha unidad, un sensor en la mayoría de los casos con elevadas prestaciones. Sin embargo, este usuario tiene la posibilidad de realizar acciones bancarias identificándose mediante su huella dactilar desde cualquier dispositivo electrónico que posea un sensor para dicha acción. Este sensor suele ser diferente al que el usuario utilizó para registrarse la primera vez, y en la mayoría de los casos suele tener peores prestaciones, lo que puede hacer que necesite varios intentos para la autentificación y que, en ocasiones, no sea capaz de mostrar al banco su identidad, lo que sería calificado como fraude e imposibilitaría la realización de cualquier acción bancaria.

Del mismo modo ocurriría en las fronteras de los países que poseen este método de identificación. Será probable que los países con mayor poder adquisitivo dispongan de sensores más precisos, con mayor calidad y mejores prestaciones que los países con un poder adquisitivo menor. Esta diferencia en los sensores puede provocar que se disminuya su rendimiento, originando errores de identificación cuando el registro de un usuario se realiza con un sensor distinto del utilizado para identificaciones posteriores. Tras la realización del estudio comprobaremos hasta qué punto varía el rendimiento de los sensores en estas situaciones.

El adquirir los conocimientos proporcionados por las prácticas y por tanto adentrarse en el mundo de la biometría, y ante las incomodidades que en los casos anteriormente mencionados proporcionan los sistemas biométricos, han hecho que el presente proyecto sea el seleccionado por la alumna, lo que hará que el tema se trate con interés personal estando siempre presente la perspectiva social.

Hoy en día, el reconocimiento biométrico de personas es un método legalmente aceptado en casi todo el mundo. Pero este método no llega hasta aquí, si no que se prevén grandes avances en esta forma de autentificación, dado que la biometría permite obtener elevada precisión y fiabilidad en los sistemas de seguridad.

1.2 Objetivos

El objetivo principal de este proyecto es conocer cómo varía el rendimiento de los sensores de huella dactilar cuando se produce el registro de un usuario en una base de datos con un sensor diferente al que dicho usuario utilizará en futuras identificaciones. Este proceso de variación recibe el nombre de interoperabilidad entre sensores.

Tras el objetivo principal se definen los siguientes objetivos específicos:

- Diseño e implementación de una aplicación con plataforma Visual Studio, capaz de procesar una base de datos de huellas dactilares recopilada con sensores de captura de diferentes tecnologías.
- Diseño y desarrollo de una aplicación capaz de obtener resultados de rendimiento a partir de los datos obtenidos en la aplicación anterior.

- Análisis de las medidas de rendimiento para las diferentes tecnologías, utilizando las aplicaciones anteriores se hará el análisis de interoperabilidad, objetivo principal de este TFG. Este análisis consistirá en dos tipos de experimentos, el primer experimento analizará el rendimiento de los sistemas cuando en todo el proceso que supone la identificación de una persona se utiliza el mismo tipo de sensor, y, el segundo, para cuando en ese proceso se utilizan sensores diferentes.

1.3 Marco socio-económico

Como se ha comentado en el apartado 1.1, Motivación, el futuro de la biometría se centra en la seguridad de los sistemas, por ello, cada vez con mayor interés, se estudian los diferentes tipos de técnicas biométricas, y las diferentes soluciones existentes para cada una de ellas.

Dentro de cada una de las técnicas biométricas se encuentran sistemas que requieren interoperabilidad entre los sensores utilizados para la captura de datos biométricos, como es el caso de la banca o de las fronteras, casos anteriormente comentados. Dada la relevancia de este problema en la actualidad, se plantea el análisis de interoperabilidad de sensores de huella dactilar como Trabajo de Fin de Grado.

Dicho análisis permitirá conocer si el grado de fiabilidad que presentan los sistemas de identificación biométrica se ve afectado por la utilización de diferentes sensores. En vista de los resultados se podrá determinar si es posible utilizar sensores más económicos o de diferentes fabricantes para una misma solución manteniendo el mismo grado de seguridad. A su vez, este parámetro puede suponer una reducción de costes significativa a la hora de reponer los sistemas utilizados en una misma aplicación basada en el reconocimiento biométrico.

1.4 Marco regulador

El presente proyecto se enmarca dentro de dos tipos de normas:

- La norma ISO/IEC19795 –Parte 1 "*Biometric performance testing and reporting- Principles and framework*"[1], necesaria para la realización de cualquier evaluación de rendimiento de sistemas biométricos. Este estándar pertenece a una serie la cuál especifica cómo planificar, efectuar y documentar las evaluaciones de rendimiento de los sistemas biométricos.

- La norma LOPD [2] "*Ley Orgánica de Protección de Datos*", necesaria para el trato de los datos personales de los usuarios participantes en la evaluación. Esta norma regula que en ninguna de las partes del análisis se revele más información que la huella dactilar de cada usuario, por ello, con el fin de cumplir la norma establecida, los datos utilizados son tratados de forma anónima.

1.5 Estructura del documento

El presente documento se encuentra dividido en 5 capítulos, a continuación se muestra un breve resumen del contenido de cada uno de ellos.

El primero, INTRODUCCIÓN, ofrece la motivación que ha conducido a la realización de este proyecto, así como los objetivos que se pretenden alcanzar. Además se proporciona el marco socio-económico y regulador donde se enmarca el proyecto.

El segundo capítulo, FUNDAMENTOS TEÓRICOS, está enfocado hacia el estudio de la biometría y de la identificación biométrica de personas mediante su huella dactilar.

El tercero, DISEÑO DE LA SOLUCIÓN, recoge los sensores utilizados en el proyecto, así como la base de datos y las modificaciones realizadas en la misma. No obstante, este apartado comprende las herramientas necesarias para la creación de las aplicaciones realizadas.

Como cuarto capítulo se encuentra la IMPLEMENTACIÓN DE LA SOLUCIÓN. Para este capítulo se reserva toda la introducción a las plataformas de desarrollo utilizadas para la creación de las aplicaciones: todo el diseño de la aplicación en Visual Studio, incluyendo todas las mejoras que ésta ha ido sufriendo desde el inicio, creándose inicialmente una aplicación de consola manual, para pasar a ser una aplicación WPF también con accionamiento manual y terminar siendo una WPF automática, y todos los detalles de la herramienta necesaria para obtener las medidas de rendimiento de los sistemas utilizados, "Biosecure Tool".

El quinto capítulo, EXPERIMENTOS REALIZADOS, se compone de todas las pruebas, experimentos, que se han realizado durante la creación del proyecto, detallando en cada una de las pruebas los pasos seguidos. Además incluye el análisis de los resultados obtenidos, separando dichos resultados en los escenarios de igualdad y de interoperabilidad.

No obstante, sin ser calificados como capítulos, se incluyen las secciones correspondientes al resumen, "abstract", conclusiones del proyecto, bibliografía y finalmente un anexo donde se incluye la planificación y presupuesto del proyecto realizado.

2. FUNDAMENTOS TEÓRICOS

2.1 Identificación biométrica por huella dactilar

2.1.1 Introducción a la biometría

La palabra biometría deriva de las palabras griegas "bios", vida y "metron", medida. Entendemos por biometría el estudio estadístico de parámetros biológicos, como pueden ser la influencia de enfermedades por sectores de la población o la propagación de insectos en los campos de cultivo [3].

La definición de biometría se hace más específica cuando utilizamos este término para referirnos al reconocimiento de personas.

2.1.2 Reconocimiento biométrico

Aplicado a los seres humanos, se entiende por biometría, el estudio de los métodos automáticos para el reconocimiento de las personas mediante la medida de sus características intrínsecas, lo que se denomina reconocimiento o identificación biométrica [4].

Hoy en día, los términos de reconocimiento biométrico o identificación biométrica se utilizan indistintamente, aunque el término de identificación biométrica, también se utiliza para definir un tipo de reconocimiento, estos conceptos serán explicados en el apartado 2.1.2.4.

2.1.2.1 Propiedades de las características biométricas

Los seres humanos poseen una serie de características intrínsecas, también denominadas rasgos, propias de cada individuo. Para que una característica pueda ser calificada como característica biométrica debe cumplir en mayor o menor medida las siguientes propiedades o requisitos, definidos por el investigador italiano Davide Maltoni en [5].

- Universalidad: todos los individuos deben poseerla.
- Unicidad: debe ser diferente para cada persona, por lo que se debe identificar unívocamente a cada individuo.
- Permanencia: debe permanecer invariable a lo largo del tiempo.
- Mensurabilidad o facilidad de captura: debe ser posible adquirirla y procesarla.
- Rendimiento: el nivel de precisión, rapidez y robustez a la hora de identificar a la persona debe ser razonable.
- Aceptabilidad: la mayoría de la población debe aceptar el método de identificación y confiar en su uso.
- Invulnerabilidad: la característica permite una robustez del sistema frente a los métodos de acceso fraudulentos.

2.1.2.2 Características intrínsecas de los humanos

Una vez definidos los requisitos a cumplir por una característica biométrica dividimos las características biométricas de los seres humanos en los siguientes dos grupos [3], [6], [7]:

- Por un lado tenemos las características físicas o características estáticas, cualidades de los humanos que permiten diferenciarles del resto de sus semejantes, como pueden ser el ADN, las huellas dactilares, la retina, el iris, los patrones faciales, de venas de las manos o la geometría de la palma de la mano. El tipo de reconocimiento biométrico que usa la medición de las características físicas para la identificación de sujetos se denomina biometría estática o morfológica. Los principales estudios de este tipo de reconocimiento biométrico se centran en el reconocimiento por ADN, por huella dactilar, por la geometría de la mano, por el análisis de iris, retina y córnea y por el reconocimiento facial.

- Por otro lado tenemos las características de comportamiento o dinámicas, referidas a las diferentes maneras de ejecutar una determinada actividad. Dicha ejecución conlleva un comportamiento adquirido o aprendido a lo largo del tiempo, como son la firma, el paso o el tecleo. El reconocimiento biométrico que mide las características de comportamiento para la identificación de sujetos se denomina biometría dinámica o de comportamiento. En este grupo los principales estudios se basan en el reconocimiento de los individuos mediante su firma manuscrita.

Por último, podemos considerar la voz como una mezcla de características tanto físicas como de comportamiento.

No todos estos tipos de reconocimiento biométrico están igual de desarrollados o son igual de fiables. En la Tabla 1 se ofrece una comparativa de los factores más determinantes en el uso de los métodos más utilizados.

Tabla 1: Factores que determinan la fiabilidad de las técnicas biométricas más utilizadas [8]

	ADN	Huellas dactilares	Firma escrita	Voz	Iris	Cara
Fiabilidad del método	Muy alta	Alta	Alta	Alta	Muy alta	Alta
Facilidad de uso	Media	Alta	Alta	Alta	Media	Alta
Prevención de ataques	Muy alta	Alta	Media	Media	Muy alta	Media
Aceptación social	Muy alta	Media	Muy alta	Muy alta	Media	Muy alta
Estabilidad	Muy alta	Alta	Media	Media	Alta	Media

Dado que la biometría se fundamenta en la medida de las características intrínsecas de cada individuo, características intransferibles que impiden en gran medida la suplantación del sujeto, podemos hablar de esta ciencia como una ciencia fiable y segura.

A continuación, se ofrece la Tabla 2, donde se numeran las diferentes tecnologías en base a los siete requisitos, definidos por Davide Maltoni, apartado 2.1.2.1, que una característica biométrica debe cumplir.

Tabla 2: Ranking de las técnicas evaluadas en base a la fiabilidad del método [4].

Puesto	Puntuación	Técnica
1º	32	ADN
2º	30	Huella Dactilar
3º	27	Reconocimiento de Iris
4º	21	Firma escrita
5º	20	Reconocimiento Facial
6º	17	Reconocimiento de Voz

En función de los datos reflejados en la Tabla 2 se puede apreciar que el reconocimiento por huella dactilar es una de las técnicas de reconocimiento biométrico más utilizadas y, por tanto, más estudiadas hasta la fecha debido a las buenas características que poseen las huellas dactilares en el campo biométrico y al gran cumplimiento de esta técnica de los requisitos descritos por Maltoni.

Dada la importancia de esta técnica de reconocimiento biométrico se ha seleccionado esta modalidad para la realización del presente TFG.

2.1.2.3 Estructura general de los sistemas de identificación biométrica

A pesar de que las técnicas de reconocimiento biométrico son muy diversas, todas ellas comparten un esquema general totalmente independiente, que consta de las siguientes dos etapas [8]:

- Reclutamiento (Modo de registro o “enrolment”).

  Es el primer paso del proceso de identificación biométrica. En esta fase se recogen una serie de muestras del usuario a identificar con sus datos característicos, el número de datos a recoger varía según la técnica a utilizar. Por un lado existen técnicas en las que únicamente es necesario recoger una muestra mientras que en otras son necesarias varias e incluso varias sesiones con un intervalo temporal variable entre ellas.

El reclutamiento en varias sesiones es necesario si el proceso es demasiado extenso y puede provocar un rechazo de la técnica por parte del usuario o su incomodidad, lo que provocaría la obtención de un patrón pésimo y en consecuencia identificaciones con bajo rendimiento.

Una vez recogidas las muestras, se procesan con el fin de generar un patrón. Éste patrón representa el conjunto de datos de caracterización del usuario y quedará almacenado en una base de datos protegida para futuras identificaciones.

La generación del patrón es una tarea delicada, ya que un patrón mal generado va a presentar un elevado número de errores en posteriores comparaciones. Es por ello que en esta etapa se necesita disponer de la supervisión de una persona, un operador, para la realización de las siguientes funciones:

- Por un lado debe comprobar la identidad de la persona a reclutar y mostrarle el funcionamiento del sistema de reconocimiento, así como resolver todas las dudas que dicho usuario pudiera tener acerca del sistema.

- Por otro lado debe decidir si las muestras recogidas son válidas para la generación del patrón del usuario, o en su defecto, si su toma es errónea o posee baja calidad. En el último caso, debe ser rechazada para pasar a recoger otra muestra válida en su lugar.

- Utilización del sistema.

Una vez que las características del usuario están recogidas en el patrón y este se encuentra almacenado en la base de datos, el usuario puede comenzar a utilizar el sistema de reconocimiento.

La función del sistema es comparar el patrón almacenado en la base de datos con el nuevo patrón generado cuando el usuario intenta identificarse. Si ambos patrones coinciden el usuario será identificado y se le permitirá realizar la acción para la cual necesitaba previa identificación, como puede ser acceder a una zona con seguridad, realizar alguna compra o simplemente desbloquear su teléfono móvil. Si por el caso contrario los patrones no coinciden, se producirá un error en la identificación y por tanto impedirá la tarea para la cual necesitaba identificarse.

Estas dos etapas generales pueden ser desglosadas en una serie de bloques o fases más concretas que permiten explicar el funcionamiento paso a paso del sistema de reconocimiento. Todas las fases se encuentran interrelacionadas para permitir el buen funcionamiento del sistema e identificar fácilmente al individuo en base a sus características biométricas. Estos bloques se encuentran organizados de la siguiente manera:

- Captura de los datos biométricos.

  Se toman muestras con el fin de obtener los datos biométricos del individuo. Estas muestras son recogidas de manera diferente en función de la técnica de identificación utilizada. Además, se pueden encontrar variantes de recogida para la misma técnica, como se verá en el apartado 2.1.3.4 para el caso de la huella dactilar.

- Pre-procesado de los datos capturados.

  Se adecuan los datos capturados para facilitar las tareas del siguiente bloque. Las tareas de adecuación de los datos dependen de la técnica utilizada, como ejemplo para el reconocimiento por voz tenemos el reconocimiento del inicio de una frase o la medida del ruido de fondo; para el reconocimiento por huella, la determinación de los bordes de la imagen capturada, la rotación o ampliación de la imagen.

- Extracción de las características del usuario.

  Se trata de la fase más significativa de cualquiera de las técnicas de identificación, ya que es el bloque en el que se basa la capacidad del sistema de distinguir a los individuos.

  Además, la importancia de esta fase recae en la creación de un fichero, donde se almacenan las características más significativas de la muestra biométrica de la persona.

- Comparación con el patrón almacenado.

  Este bloque se utiliza únicamente en la etapa de utilización del sistema. Una vez se extraen las características de la muestra capturada, se procede a la generación de un nuevo patrón correspondiente a dicha muestra, por lo que cada vez que un usuario se identifica en el sistema se extraen las características de la muestra proporcionada. Dicha muestra es comparada con la almacenada en la base de datos, BBDD, para determinar si se trata del mismo usuario. A la muestra de datos almacenada en la BBDD se la suele denominar patrón.

  El éxito o el fracaso de la comparación está condicionado por un valor umbral previamente determinado, ya que las comparaciones se realizan mediante probabilidad de semejanza, no de igualdad. Este método basado en la semejanza es necesario dado que se pueden producir leves variaciones en las características del usuario en diferentes tomas, como podría ser un pequeño corte en la yema del dedo o una leve rotación de éste en el sensor.

La seguridad del sistema viene determinada por el valor umbral, concepto que se ampliará en el apartado 2.1.3.5.

Todas las modalidades de reconocimiento biométrico siguen las mismas fases de ejecución con pequeñas diferencias, por ello se especifican las fases de ejecución para la modalidad de huella dactilar en el apartado 2.1.3.4.

2.1.2.4 Diferencia entre identificación y verificación

Hasta el momento hemos estado hablando únicamente de reconocimiento biométrico, sin embargo, la metodología del reconocimiento biométrico está dividida en dos procesos diferentes [8]:

- Identificación biométrica(1: N), también llamada reconocimiento biométrico en algunas ocasiones.

  Se basa en identificar a un usuario de los demás que se encuentran reclutados en la BBDD, por lo tanto, se comparan las características extraídas del usuario a identificar con los patrones de los demás usuarios almacenados en el sistema. El resultado puede ser positivo, si el resultado ha dado una probabilidad de semejanza por encima del valor umbral, o negativo, si el resultado ha quedado por debajo de dicho valor.

Este esquema de funcionamiento es muy utilizado por muchas aplicaciones, necesita disponer de una BBDD de patrones y una red de comunicaciones siempre on-line, cuyo fin sea la comunicación de los puestos de identificación con la BBDD.

- Verificación biométrica (1:1), también recibe el nombre de autenticación biométrica.

  Este proceso trata de comprobar si el sujeto es la persona que dice ser. Para ello cuando el usuario se recluta en el sistema entrega también su identidad, entonces, el sistema solamente comparará las características extraídas del usuario a autentificar con el patrón del mismo usuario reclutado en la base de datos. De la misma manera, si el resultado supera un umbral el usuario será quien dice ser, y si por el contrario, el resultado no supera dicho umbral se tratará de un impostor.

En la Figura 1 se puede observar de manera más intuitiva las diferencias entre identificación y verificación biométrica.

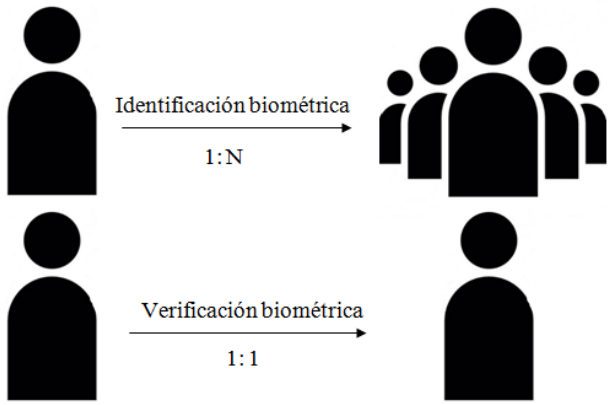


Figura 1: Concepto de identificación y verificación biométrica.

El proceso de verificación es más rápido que el de identificación, ya que solo se realiza una comparación, la de la muestra recogida con el patrón del usuario a verificar. Sin embargo, en la identificación se tiene que comprobar la muestra recogida con el patrón de todos los usuarios almacenados en la BBDD hasta encontrar el usuario al que corresponde dicha muestra, lo que supone un aumento del tiempo en proporción al tamaño de la BBDD [9].

2.1.2.5 Ventajas y desventajas del reconocimiento biométrico

Se puede afirmar que ninguna de las técnicas de reconocimiento biométrico es perfecta e ideal en todos los casos, sin embargo, ofrecen muchas ventajas, que aparecen en mayor o menor medida según la técnica. Estas ventajas se encuentran referidas frente a los sistemas de identificación tradicionales, los cuales se pueden dividir en dos grupos [10]:

- Por un lado tenemos los mecanismos basados en la posesión física de elementos, también son denominados "tokens". Aquí podemos incluir las llaves, DNIs, pasaportes, tarjetas, etc.

- Por otro lado están los mecanismos basados en el conocimiento de información secreta, esta información debe ser conocida únicamente por las personas adecuadas. De este grupo destacan las claves personales, contraseñas o los números PIN.

A pesar de que los métodos clásicos se utilizan actualmente en una gran variedad de aplicaciones, es cierto, que cada vez más, están siendo sustituidos por los métodos de reconocimiento biométrico debido a las grandes ventajas que ofrece la biometría en el campo de la identificación [4], [11].

Como principal ventaja se destaca la unicidad de los sistemas biométricos, la biometría permite identificar a un individuo dado que no existen dos características biométricas iguales en individuos diferentes.

También se destaca la comodidad. Los elementos de reconocimiento biométrico forman parte de la persona, no se trata de un elemento externo a ésta, por lo que su pérdida es imposible, a no ser que se produzca la pérdida de la parte del cuerpo donde se encuentra la característica biométrica.

Otra de las ventajas de la biometría es la seguridad que estos sistemas ofrecen, ya que a diferencia de un elemento externo, las características biométricas no pueden ser olvidadas y resultan difíciles de falsificar.

El reconocimiento biométrico no necesita mantenimiento alguno, al no disponer de ningún dispositivo externo que necesite renovación, reparación o mantenimiento, por lo que otra de las ventajas a destacar es la economía.

Otra ventaja que ofrece la biometría es que permite determinar si una persona ha sido registrada más de una vez en un sistema, como si tiene varios DNIs o varios carnets de conducir con diferentes identidades. También puede ser posible averiguarlo con los métodos clásicos pero su dificultad es mucho mayor, siendo en algunos casos imposible. Esta ventaja no solo determina el fraude, sino que, en algunos casos lo evita, ya que tener que enfrentarse a un sistema de reconocimiento biométrico suele ser suficiente para abandonar la idea de registrarse varias veces con diferentes identidades [10].

Pero, como todos los métodos de identificación, también existen algunas desventajas frente a los métodos clásicos.

La primera desventaja a destacar son las medidas de prevención. Al ser la biometría una técnica de identificación con menor recorrido que las contraseñas o tarjetas, las medidas contra los ataques a sistemas protegidos son más reducidas dado que todavía se están generando.

También se nombra como desventaja la limitación de los rasgos biométricos, cuya regeneración es imposible, a diferencia de las contraseñas o tarjetas cuya generación es ilimitada.

Teniendo en cuenta estas limitaciones, hoy en día se opta por soluciones intermedias donde la biometría suele ser combinada con los métodos clásicos, tanto contraseñas como tarjetas inteligentes, lo que proporciona potentes herramientas para la identificación personal.

2.1.2.6 Grado de aceptación en la sociedad

La aceptación por parte de la sociedad de cualquier nuevo sistema a instalar es un factor clave para el éxito o el fracaso del mismo. En el caso del reconocimiento biométrico todas y cada una de las técnicas cuentan, en mayor o menor medida, con partidarios y detractores [4]. No cabe duda que la identificación biométrica se ha extendido gracias a la aceptación social de los usuarios, quienes han encontrado ventajas en este sistema frente a los métodos de identificación tradicionales.

Hoy en día, son cada vez más las acciones que requieren la identificación de personas, esto supone una muestra de aceptación por parte de los usuarios, quienes aceptan o rechazan libremente el uso de dicha tecnología.

Es tal la aceptabilidad de algunas de estas técnicas, que numerosas personas ya las utilizan en su vida diaria. Ejemplo de ello puede ser la huella dactilar, ya que algunos “Smartphones” llevan integrado un sensor de huella dactilar que permite o deniega el acceso al teléfono, lo que asegura que solo la persona registrada en dicho teléfono tendrá acceso a él.

También existen técnicas que son utilizadas por la aceptación histórica del método. Ejemplo de ello puede ser la firma manuscrita, ésta lleva utilizándose como método de identificación durante muchos años ya que no deja ningún rastro más por parte de la persona, este método es aceptado universalmente en operaciones gubernamentales, legales y comerciales. Todo esto hace que esta técnica goce de buena aceptación por parte de los usuarios.

Es de vital importancia tener en cuenta el papel de la aceptación cultural a la hora de implantar la biometría como sistema de identificación. El ámbito cultural puede suponer un inconveniente en determinados países en los que existen unas normas sociales y religiosas no favorables a la toma de las muestras biométricas necesarias. Se puede nombrar el caso de las culturas en las que el reconocimiento facial se hace dificultoso dado que no todos los ciudadanos llevan el rostro descubierto; también se da el caso de las culturas que consideran una práctica antihigiénica la lectura de la huella dactilar [12].

2.1.3 Introducción al reconocimiento biométrico mediante huella dactilar

De todas las características morfológicas únicas que tenemos los humanos, en este periodo, nos hemos volcado en el estudio de la biometría mediante el análisis de la huella dactilar.

Para poder profundizar en el reconocimiento de los humanos a través de la misma y poder comprender en qué consiste dicha identificación, tenemos que conocer que es una huella dactilar, así como sus características respecto a la identificación.

2.1.3.1 Definición y características de la huella dactilar.

Se define como huella dactilar, la impresión visible o moldeada que produce el contacto de las crestas papilares de un dedo de la mano sobre una superficie [13]. Un ejemplo de una huella dactilar se muestra en la Figura 2.

Figura 2: Impresión de una huella dactilar sobre una superficie [14].

Una huella dactilar aparece como una serie de líneas oscuras, las cuales representan los relieves (saliente de las crestas de fricción), que contrastan con espacios en blanco, correspondientes a los valles (bajo relieve) situados en las yemas de los dedos (Figura 3).

Figura 3: Definición gráfica de una huella dactilar [15].

Se califica como reconocimiento biométrico a la identificación de personas mediante su huella dactilar ya que la característica utilizada, la huella dactilar, cumple con los siete requisitos determinados por el investigador italiano Davide Maltoni, comentados en el apartado 2.1.2.1:

- Se dice que las huellas dactilares son universales, ya que todo el mundo debe poseerlas.
- Son perennes, pues son formadas en sexto mes de la vida intrauterina, e invariables en número, situación, forma y dirección hasta la putrefacción de la piel.
- También son inmutables, es decir, las crestas papilares no pueden modificarse fisiológicamente, si se produce un traumatismo poco profundo, las crestas se regeneran. Si se trata de un traumatismo profundo la parte afectada queda invadida por un dibujo cicatrizal.
- Las huellas dactilares también poseen una característica llamada unicidad, esto significa que cada huella es diferente en cada persona, todavía no se han hallado dos impresiones idénticas en dedos diferentes
- Tienen un elevado grado de comodidad a la hora de la adquisición.
- Las personas poseen un elevado número de fuentes disponibles para su recolección, ya que existe una fuente de recolección por cada dedo.
- Por último decir que el código biométrico nunca se olvida, pues la persona siempre lo lleva consigo. Se trata de una gran ventaja frente a otros métodos de identificación como códigos alfanuméricos.

2.1.3.2 Historia de las huellas dactilares.

Desde la antigüedad se han identificado a las personas mediante diferentes partes de su cuerpo, una de las características más utilizada para el reconocimiento es el rostro, desde los inicios de la historia los humanos han reconocido a sus familiares o conocidos mediante los rasgos de sus rostros.

Existen numerosas evidencias arqueológicas que relacionan huellas con identidad [4], [16], prueba de ello son las antiguas cuevas descubiertas con pinturas en su interior, supuestamente realizadas por hombres prehistóricos quienes habitaron en ellas. Estas pinturas contaban con numerosas impresiones de manos o dedos que actuaban como firmas con el fin de identificar a sus creadores.

Sin embargo, no solo se han encontrado huellas dactilares a modo de firma en pinturas antiguas, sino que también han sido encontradas impresiones de huellas dactilares en pastillas de arcilla en el ámbito de las transacciones comerciales. Estas eran utilizadas como método de identificación de los comerciantes y comenzaron a utilizarse por los babilonios alrededor del año 500 AC.

A mediados de 1800, con el crecimiento de la población se incrementan los delitos, por lo que la justicia demanda un método donde se pudiese identificar a los infractores, con el fin de aplicar mayores castigos a aquellos que fuesen reincidentes. Esto se solucionó con la creación de unas tarjetas donde se recogían algunos de los parámetros físicos de los infractores, como podía ser la altura o la longitud de sus brazos y piernas.

El revolucionario sistema de identificación mediante la huella dactilar fue inventado por Juan Vecetich. Este método se basaba en un rasgo físico mucho más individual y personal que los recogidos en las tarjetas que hasta entonces se utilizaban. Nacido en la actual Croacia, Vecetich desarrolló y patentó su sistema en Argentina. Hizo las primeras fichas dactilares del mundo con las huellas de 23 procesados, este suceso tuvo lugar el 1 de Septiembre de 1891, día que quedó reconocido como día mundial de la Dactiloscopia, ciencia sobre la que se basa el reconocimiento de huellas dactilares.

El primer caso policial resuelto gracias a la utilización del sistema de Vecetich fue en 1892 en Argentina. En él, se involucraba a una mujer de nombre Francisca Rojas en el asesinato de sus dos hijos, evidencia que quedó demostrada tras comparar las huellas de Francisca con las huellas latentes encontradas en el arma. Una muestra de las huellas tomadas a esta mujer puede verse en la Figura 4. Más tarde se empleo el mismo método de comparación de huellas dactilares para verificar a 645 reclusos de la cárcel de La Plata y, tres años más tarde la Policía de Buenos Aires adoptó oficialmente su sistema [17].

Finalmente, en 1924 se instauró como método de identificación del FBI las huellas dactilares [18].

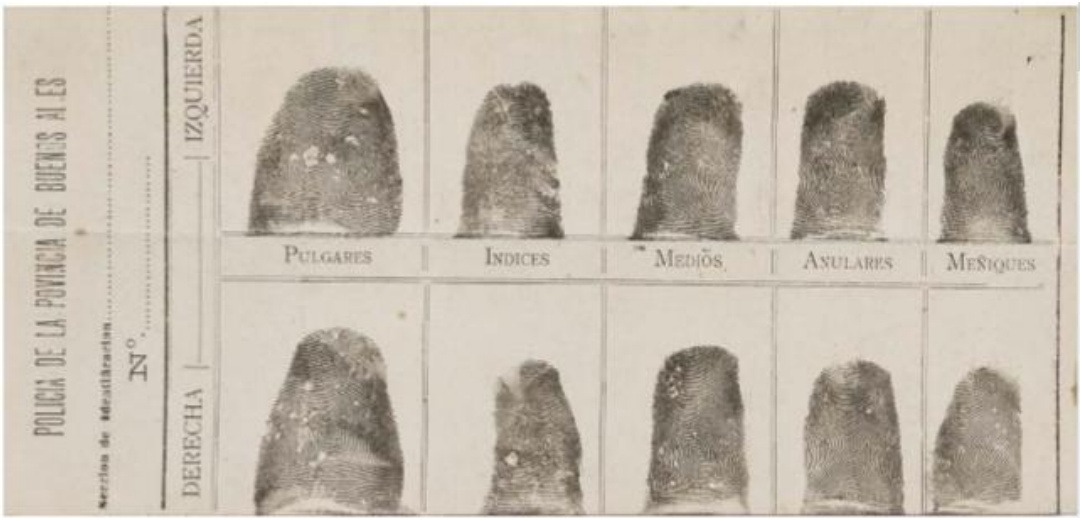


Figura 4: Ficha dactiloscópica de las huellas de Francisca Rojas [19].

Sorprendentemente el reconocimiento biométrico mediante huella dactilar ya era utilizado en China y Japón unos 1200 años atrás, cuando los padres chinos comenzaron a utilizar las impresiones de dedos y pies de sus hijos con el fin de diferenciarlos [20].

El primer estudio científico publicado sobre la estructura de crestas, valles y poros de las huellas dactilares data de 1684, realizado por el morfologista inglés Nehemiah Grew [18].

2.1.3.3 Evolución de las aplicaciones de identificación mediante huella dactilar.

El uso de las huellas dactilares ha evolucionado desde las primeras aplicaciones anteriormente comentadas, como podían ser la impresión de la palma de la mano o de un dedo en una pintura rupestre, con el fin de identificar al creador; la impresión de la huella dactilar como firma de los comerciantes; más tarde la impresión de una huella en cualquier creación de arcilla, como vasijas o las impresiones de los pies de los niños chinos en papel, etc, hasta la utilización de dicho rasgo biométrico en el ámbito policial, principalmente.

Uno de los principales avances del reconocimiento biométrico fue la introducción de la huella dactilar en el DNI, ya que esto permite la identificación unívoca de las personas, dado que todas ellas poseen dicho documento de identidad.

Gracias al avance de las capacidades de computación, la huella dactilar ha cambiado su forma de captura, dejando atrás su obtención en papel y dando lugar al nacimiento de la huella digital obtenida a través de sensores electrónicos.

No debemos confundir huella digital con huella dactilar (Figura 5), ya que la huella digital es la captura de la huella dactilar mediante un dispositivo electrónico, el cual suele ser denominado sensor de huella digital (Figura 6); una vez que el sensor captura la huella esta es traducida a una serie de bits.

Figura 5: Ilustración de una huella digital [21].

Figura 6: Ilustración de un sensor de huella dactilar [22].

Por lo que de ahora en adelante cuando se nombre la huella dactilar nos estaremos refiriendo a la huella dactilar tomada con un sensor electrónico, es decir, a la huella digital.

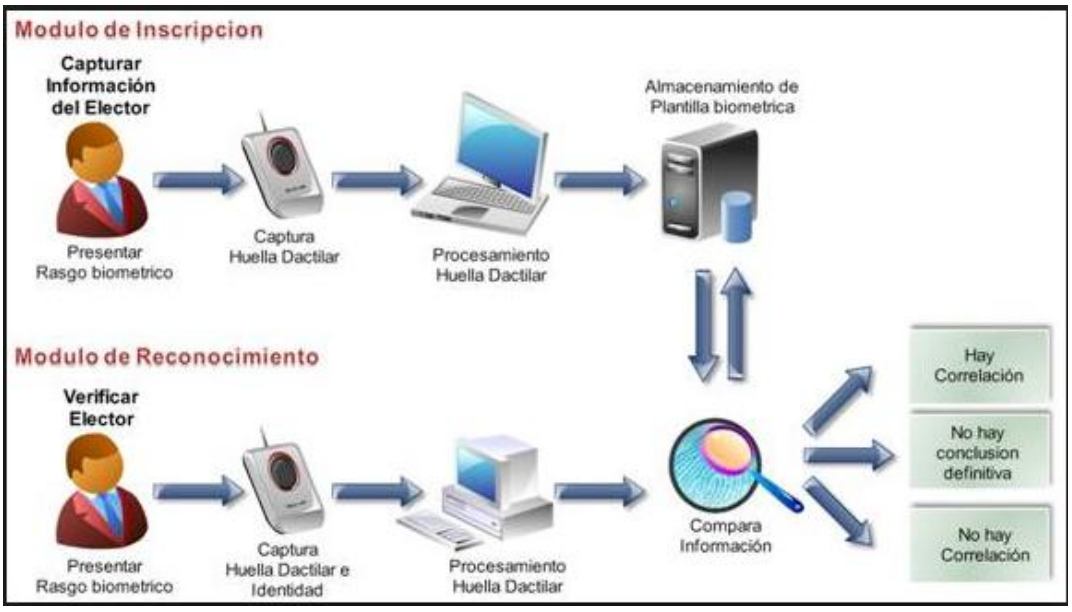
Gracias al avance de la computación, al empleo de nuevas tecnologías, a la mejora del uso de escáneres y al procesado digital de imágenes, las aplicaciones que cuentan con el método de identificación mediante huella dactilar no se encuentran restringidas únicamente al ámbito policial, sino que, son numerosos los campos y ámbitos que encuentran en este método una forma de identificación personal segura y fiable.

Además, el nacimiento de la huella dactilar automática, huella digital, ha favorecido el procedimiento de extracción de las características propias de cada persona situadas en la huella, haciéndolo más rápido, preciso y fiable.

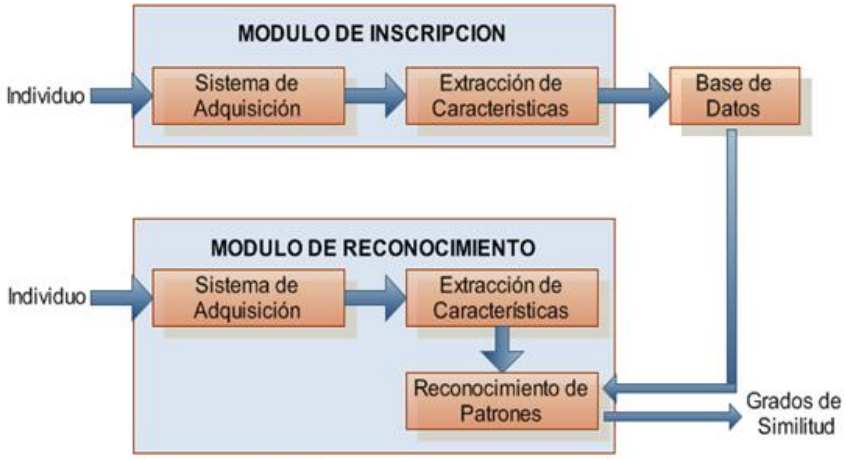
El crecimiento del uso de este tipo de identificación es debido a la gran riqueza de información que se puede obtener en cada dactilograma, entendiendo por dactilograma, el conjunto de figuras que se forman por el relieve de las crestas papilares del dedo [4].

2.1.3.4 Fases del reconocimiento biométrico mediante huella dactilar.

Como se ha comentado en el capítulo 2.1.2.3 todas las técnicas de identificación biométrica siguen el mismo esquema con alguna variante, en el caso de las huellas dactilares es muy semejante el esquema que sigue el proceso de identificación y el de verificación, dicho esquema se detalla a continuación (Figura 7).



(a)



(b)

Figura 7: Proceso de reconocimiento biométrico [23].

(a) Esquema de un sistema de reconocimiento biométrico.
(b) Diagrama de bloques de un sistema de reconocimiento biométrico.

Dentro del proceso de reclutamiento se encuentran las siguientes fases:

- Segmentación: etapa en la que se localiza la parte de la imagen donde se encuentra la información útil, descartando el resto de la captura.

- Extracción de minucias de la imagen: etapa en la cual se determinan los puntos característicos, minucias, de una captura.

Para la identificación por huella digital debemos conocer previamente algunas posibilidades de puntos característicos, representados en la Figura 8:

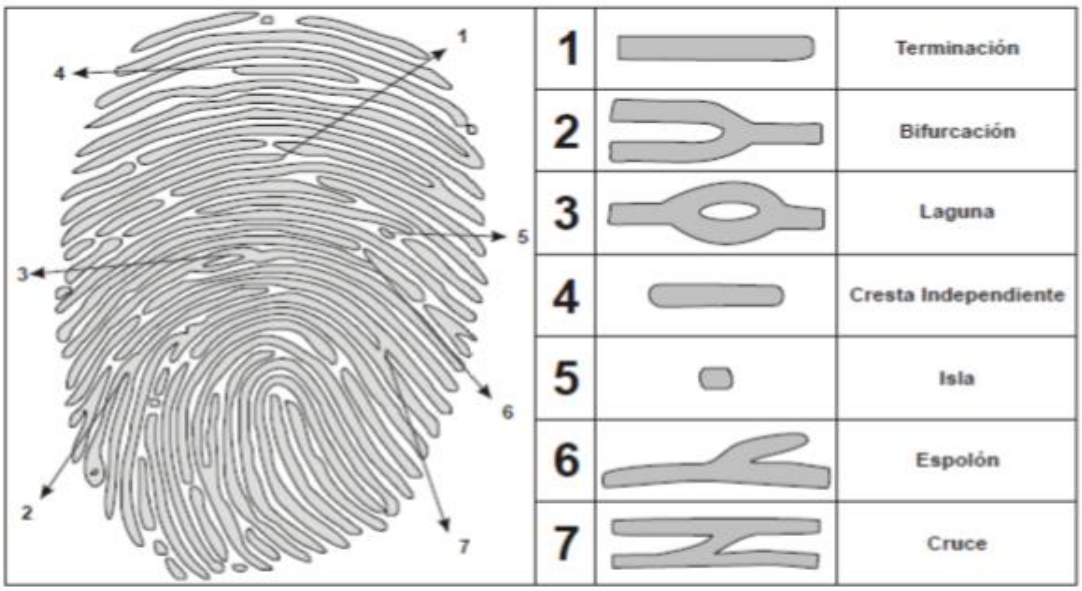


Figura 8: Diferentes posibilidades de puntos característicos (minucias) [24].

Se entiende por minucias los puntos donde una cresta interactúa con las demás (Figura 9). Una minucia de esta imagen sería el final de una cresta, remarcado con un círculo, o la bifurcación de una cresta, minucia localizada con un rombo.

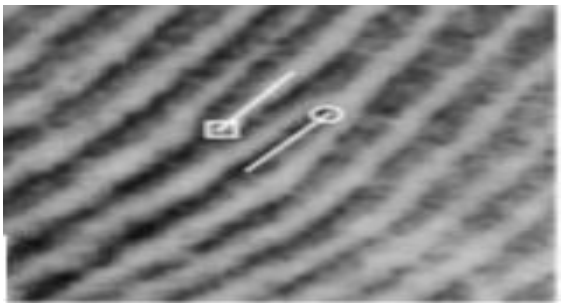


Figura 9: Ilustración real de dos minucias [25].

- Control de calidad: Las imágenes deben mostrar una buena calidad, este dato es proporcionado por un algoritmo el cual se encarga de decidir si la imagen tiene buena calidad y por lo tanto posee buena información o si por el contrario la imagen es de mala calidad y presentará un número elevado de errores en futuras comparaciones.

Una vez el usuario procede a realizar el reclutamiento, tras haber pasado las tres fases mencionadas anteriormente, si el algoritmo determina una buena calidad de imagen este patrón se almacena en la BBDD, si por el contrario la imagen es calificada con una calidad pésima, se debe proceder a la eliminación de dicha imagen y a la captura de otra muestra hasta que se alcance la calidad óptima para la generación del patrón.

Existen ocasiones en las que tras haber agotado los intentos destinados a la captura de la imagen para la generación del patrón, el usuario no ha sido capaz de conseguir una imagen con calidad aceptable, entonces se produce un error de tipo FTE "Failure to Enrol rate" y el patrón de dicho dedo no queda registrado en la BBDD.

Una vez el usuario se registra en el sistema ya puede proceder a identificarse o verificarse según cuál sea el fin.

Cualquiera de los dos procesos, identificación o verificación, sigue los mismos pasos que el reclutamiento, es decir, se genera un patrón siguiendo las tres fases comentadas anteriormente. Tras esto se produce la comparación, si se trata de identificación, el nuevo patrón generado se comparará con todos los almacenados en la BBDD y si por el contrario se trata de verificación, únicamente se comparará con el del propio usuario registrado en la BBDD.

Las comparaciones entre patrones se realizan por semejanza, siendo el valor umbral anteriormente fijado, el que determina como de semejantes tienen que ser las imágenes comparadas para que la identificación se dé por válida o no.

2.1.3.5 Medidas de rendimiento de una evaluación biométrica.

Una evaluación de rendimiento biométrico se basa en el estudio de la precisión y de la velocidad de un sistema biométrico, por lo que para analizar el rendimiento de este tipo de sistema y la interoperabilidad de los mismos nos basamos en los siguientes parámetros:

- Tasas de error. Sirven para cuantificar la precisión, ya que miden el número de errores que ocurren durante los procesos de identificación y dependen del proceso que se esté ejecutando en cada momento.

  - Durante el reclutamiento se obtienen los errores denominados FTE "Failure to Enrol rate", los cuales miden la proporción de usuarios para los cuales el sistema falla al realizar el reclutamiento.

  - Del mismo modo durante el reconocimiento se generan errores del siguiente tipo:

    - FTA "Failure to Acquire rate", los cuales miden la proporción de intentos de reconocimiento para los cuales el sistema falla al intentar adquirir muestras con suficiente calidad.
    - FNMR "False Non-Match Rate", el cual mide la proporción de intentos de reconocimiento de genuinos para los cuales el sujeto es rechazado cuando debería ser aceptado al tratarse de un usuario genuino.
    - FMR "False Match Rate", el cual mide la proporción de intentos de reconocimiento de impostor para los cuales el sujeto es aceptado y debería haberse rechazado al tratarse de un usuario no registrado en el sistema.

      Es importante mencionar que los errores FNMR y FMR están relacionados y dependen de los umbrales de decisión definidos para el sistema. Es por ello que una medida muy importante de rendimiento es el EER "Equal Error Rate" definido como el valor para el que la tasa FNMR es igual a la tasa FMR.

  - Para el caso de la verificación, también se suelen proporcionar medidas conjuntas de todo el proceso de reconocimiento, en el que se incluyen tanto los errores de captura como los de comparación. Para este caso se definen dos tipos errores:

    - FRR "False Reject Rate" o tasa de falso rechazo donde se mide la proporción de transacciones genuinas para las cuales el sujeto es rechazado cuando debería haberse aceptado.

    - FAR "False Accept Rate" o tasa de falsa aceptación, donde se miden la proporción de transacciones de impostor para las cuales el sujeto es aceptado y debería haber sido rechazado.

En este caso también existe el valor EER "Equal Error Rate" pero se define como el punto en el que la tasa FRR es igual a la tasa FAR.

Tanto para el caso de la FNMR/FMR (Figura 10) como para el caso de la FRR/FAR este punto se elige en función de la seguridad requerida.

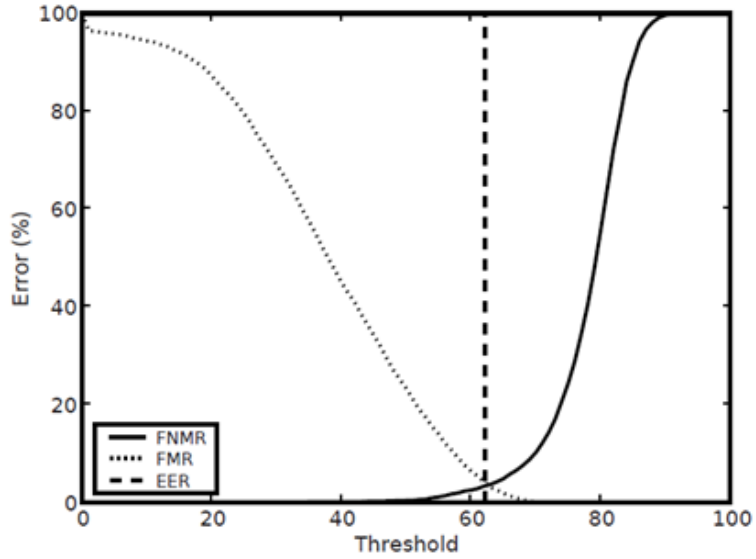


Figura 10: Gráfica FNMR frente FMR [26].

Otra de las gráficas importantes para cuantificar el rendimiento es la que se muestra en la Figura 11 .En esta gráfica se pueden observar los diferentes tipos de errores mencionados, así como la densidad de probabilidad en función de la porción de errores cometidos por el sistema, tanto dando por válida la identificación de un impostor como dando por errónea la identificación de un genuino. El nivel de seguridad se establece mediante la determinación del valor umbral o Threshold.

Si necesitamos una seguridad elevada deberemos desplazar el punto umbral a la izquierda ya que este desplazamiento implica:

- Una reducción del número de aceptados.
- Una reducción del porcentaje de errores FMR, que hace reducir el número de intentos para los que un sujeto impostor es aceptado. Esto implica que se produce un aumento en el porcentaje de errores FNMR, para los que un sujeto genuino es rechazado.

De lo contrario, si necesitamos una seguridad menos estricta debemos desplazar el punto umbral a la derecha, lo que permite aumentar la aceptación de la identificación de sujetos impostores, ya que aumenta el número de aceptados. A diferencia del caso anterior en esta situación se produce un aumento de los errores FMR y una reducción de los errores FNMR.

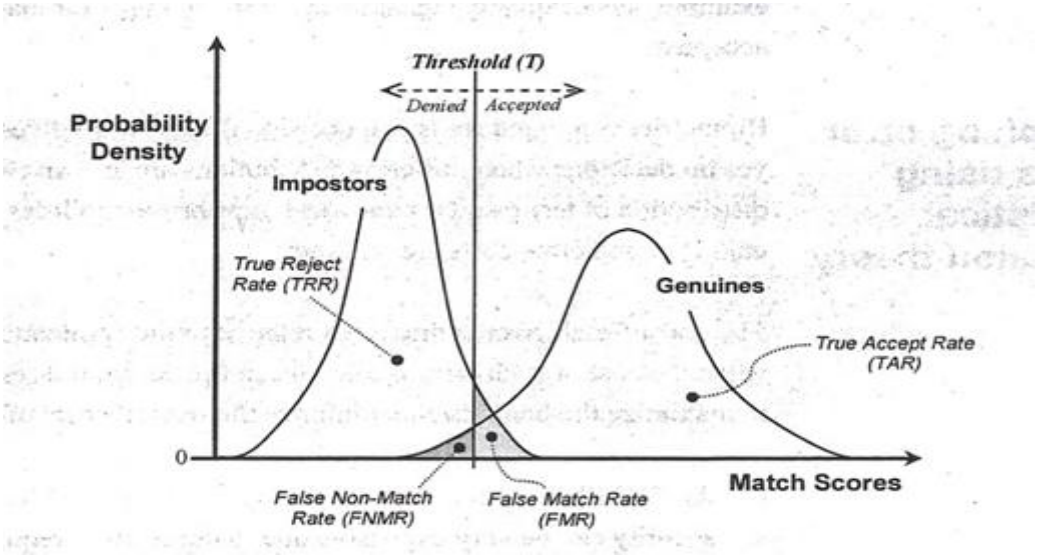


Figura 11: Concepto de valor umbral [27].

- Tasas de throughput. Estas tasas miden el tiempo que se tarda en realizar cada uno de los procesos, es decir, miden el número de usuarios que el sistema es capaz de procesar en un determinado tiempo. Estas medidas consideran tanto la velocidad de procesamiento que tiene el sistema, como el tiempo que emplea el usuario con el sistema.

  - Tiempo de reclutamiento.
  - Tiempo de reconocimiento, donde se puede separar en:
    - Tiempo de captura de la huella.
    - Tiempo de comparación de la huella capturada con el patrón generado.

2.1.3.6 Interoperabilidad de los sensores de huella dactilar

Según el instituto de Ingenieros Eléctricos y Electrónicos (IEEE) la interoperabilidad se define como "la habilidad de dos o más sistemas o componentes para intercambiar información y utilizar la información intercambiada".

Aplicado a la biometría se define como interoperabilidad entre sensores de huella dactilar, la capacidad de los sensores de intercambiar y utilizar información que no ha sido capturada o generada por ellos mismos, sino que proviene de un sensor diferente, es decir, la capacidad de un sensor para reconocer una captura de una huella que no ha sido capturada por él, sino que ha sido capturada por otro con la misma, o diferente, tecnología.

Uno de los principales problemas de las aplicaciones que utilizan la biometría automática ha sido la falta de normalización o estandarización de los sensores, de las BBDD o de los propios sistemas de reconocimiento biométrico. Esto suponía un problema ya que todos estos elementos necesarios para la identificación eran proporcionados por distintos fabricantes y con diferentes tecnologías o formatos, lo que imposibilitaba cualquier tipo de interoperabilidad entre sistemas [9].

Al paso del tiempo se han realizado mejoras en los dispositivos por parte de los fabricantes, con el fin de estandarizar los distintos formatos generados por los sistemas de captura, a diferencia de los escasos logros conseguidos en la estandarización de los algoritmos utilizados para el reconocimiento, donde la estandarización sigue siendo aún muy reducida.

Actualmente la mayor parte de los sistemas biométricos asumen, de cara al algoritmo de comparación, que las capturas se toman con el mismo sensor, esto provoca que la capacidad de reconocimiento, el rendimiento, varíe cuando los sistemas utilizados para las capturas de datos son diferentes [28]. Resultados que se comprobarán tras la realización del proyecto en el apartado de análisis de los resultados.

3. DISEÑO DE LA SOLUCIÓN

3.1 Introducción

Con motivo del problema actual de la interoperabilidad entre sensores de huella dactilar comentado anteriormente, se ha realizado el presente proyecto, donde la tarea principal es obtener resultados de rendimiento para sistemas compuestos de dos sensores diferentes, con los que poder realizar un posterior análisis de interoperabilidad. Para ello, se dispone de una base de datos con imágenes de 50 usuarios recogidas con diferentes sensores, los detalles de esta base de datos se mostrarán en el apartado 3.3.

Con el fin de alcanzar el objetivo principal, las imágenes que conforman la base de datos se han comparado varias veces, con motivo de satisfacer las pruebas necesarias. Para realizar dichas comparaciones se ha creado una aplicación mediante la plataforma Visual Studio, donde ha sido necesario incluir un algoritmo de reconocimiento biométrico de huella dactilar, NBIS, este algoritmo será extendido en el apartado 3.4.

Una vez se obtienen los resultados en la aplicación anterior, se procede a desarrollar la segunda aplicación, destinada a obtener las medidas de rendimiento de las diferentes pruebas realizadas. Esta segunda aplicación se desarrolla en Matlab y utiliza, como herramienta para la obtención de las medidas de rendimiento, "Biosecure Tool", cuyos detalles se exponen en el apartado 3.5.

Se ofrece la Figura 12, con el fin de ofrecer una perspectiva visual del diseño del experimento.

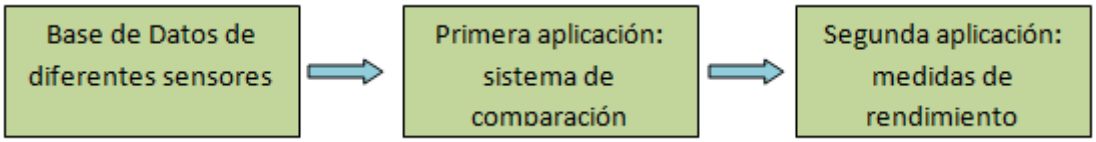


Figura 12: Diseño del proyecto.

A continuación, se detallan, en primer lugar los sensores utilizados, posteriormente tanto los detalles de la base de datos utilizada en el proyecto, como los proyectos o herramientas que han sido utilizados como referentes para la elaboración de las dos aplicaciones comentadas. Por último, se detallarán brevemente las plataformas de desarrollo

3.2 Sensores de huella dactilar

Antiguamente las huellas dactilares se recogían mediante su impresión en papel y se comparaban manualmente, determinando las minucias de las dos huellas a comparar y observando cuales de ellas eran iguales en ambas impresiones. Sin embargo, gracias al avance de la tecnología, los métodos de recolección y comparación han ido evolucionando, dejando atrás el papel para dar paso al sensor de huella dactilar.

3.2.1 Definición de sensor de huella dactilar

Se trata de un dispositivo electrónico encargado de detectar los relieves de la yema del dedo mediante la utilización de luz o por medio de sensores eléctricos, y tras ello generar una imagen digital, es decir, transforma la imagen dactilar recogida a una serie de bits, dicha imagen es enviada al ordenador y almacenada en una BBDD asociándola con la información de la persona a la que pertenece [29].

3.2.2 Tipos de sensores utilizados en el estudio

Para el presente análisis de rendimiento experimental se han utilizado tres sensores, uno de ellos un sensor térmico y los otros dos capacitivos, a continuación se detallan sus características, así como su principio de funcionamiento:

3.2.2.1 Sensor térmico

Concretamente ha sido utilizado el sensor térmico NB-3010-U (NXT).

Este sensor obtiene las imágenes de las huellas dactilares mediante las diferentes temperaturas de la yema del dedo (Figura 13), gracias a la posesión de material piroeléctrico, éste convierte la diferencia de temperatura en diferencia de tensión.

El calor de la yema del dedo aumenta cuando hay una cresta y por el contrario se reduce cuando se encuentra con un valle. Cuando se coloca el dedo en el área activa del sensor el calor conducido por la yema del dedo se traduce a una serie de bits que representan diferentes niveles de grises con el fin de formar una imagen digital.

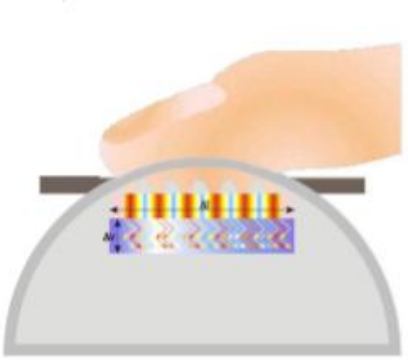


Figura 13: Funcionamiento de un sensor térmico [4].

3.2.2.2 Sensor capacitivo

Como sensores capacitivos se han utilizado el FPC1011F3 (FPC) y el UPEK Eikon Touch 51 (UPK)

El funcionamiento de los sensores capacitivos (Figura 14) se basa en la posesión de condensadores, los cuales varías su capacidad al colocar el dedo en la superficie del sensor. Concretamente, la capacidad se reduce más cuando en la superficie se detecta una cresta que cuando se detecta un valle.

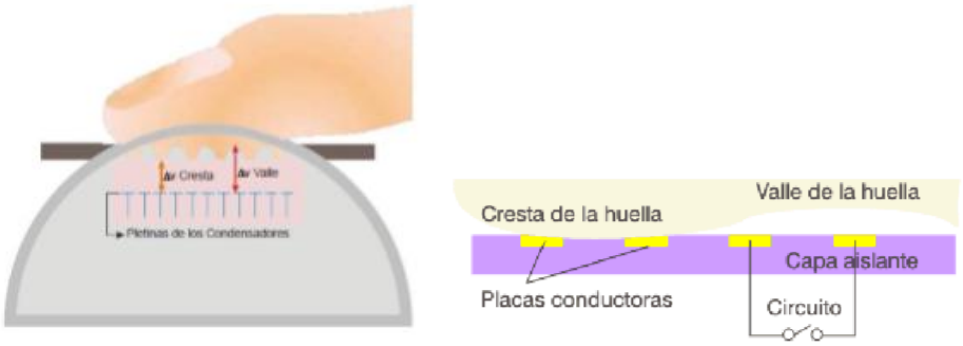


Figura 14: Funcionamiento y circuito de un sensor capacitivo [4], [30].

3.3 Base de datos

Para la realización de este proyecto ha sido necesaria una base de datos de huellas dactilares, por lo que se ha utilizado parte de la base de datos generada durante la evaluación biométrica realizada en el periodo de realización de las prácticas de empresa que se describió en el apartado 1.1. A continuación se describen los detalles de la base de datos recopilada.

Para la realización de una evaluación biométrica es necesario recoger un gran volumen de muestras, por lo que se contó con la participación de 580 usuarios, quienes fueron presentados voluntariamente para prestar su colaboración en la evaluación, cuyo fin era la comparación de tres sensores de huella dactilar. La formación de la base de datos se produjo en dos visitas por cada usuario.

En la primera el usuario era registrado en el sistema (reclutamiento o enroll), entregando su identidad, así como características que tienen influencia en los datos biométricos, como puede ser la edad, el sexo o la lateralidad de cada usuario. Tras el reclutamiento el usuario pasaba a tratar de verificarse en el sistema, volviendo a colocar numerosas veces los dedos a estudiar en los tres sensores diferentes. Una vez el usuario iba colocando los dedos en los sensores, el sistema determinaba si la nueva huella guardaba semejanza con el patrón del reclutamiento almacenado previamente en la base. Si era así, el usuario era reconocido como genuino y se pasaba a la comparación del siguiente dedo. De no ser así, el sistema entregaba un error dando la oportunidad de volver a colocar el dedo en dicho sensor hasta un total de 3 intentos.

La posibilidad de realizar tres intentos se debe a que es de gran importancia tener una buena colocación del dedo en el sensor, ya que cualquier rotación o movimiento del dedo puede provocar que el sistema no determine semejanza en las huellas aun tratándose de un genuino, como se extenderá en el apartado 3.4.1.1.3.

Si tras los tres intentos el usuario no era capaz de verificarse se pasaba al siguiente dedo, y así, sucesivamente. Tras el reclutamiento y la primera identificación el usuario debía volver a realizar una segunda verificación, del mismo modo que se realizó la primera, pasados un mínimo de 15 días.

El periodo de espera entre la primera visita y la segunda es debido a la búsqueda de comparaciones óptimas, ya que como se explicó en el apartado 2.1.2.3 una sesión de larga duración puede provocar cansancio en el usuario y por tanto rechazo al método o capturas de mala calidad. Además, 15 días es el tiempo que tarda cualquier corte sin profundidad en regenerarse, y el tiempo en el que el usuario olvida el funcionamiento del método.

Esta última idea se basa en que cuando un usuario ha trabajado con este tipo de sensores obtiene mejores resultados que los de un usuario sin conocimientos acerca del método, de lo que se puede afirmar que el rendimiento mejora según aumenta el uso de este tipo de sistemas. Es por ello que se le pide al usuario que acuda a proporcionar sus huellas en más de una ocasión.

De los 580 usuarios que fueron estudiados en la evaluación para este proyecto se han utilizado los 50 primeros, de los cuales no se posee ningún tipo de información más que las imágenes de las huellas dactilares de sus dedos, índice, corazón y pulgar de ambas manos, incluyendo en la base las imágenes de reclutamiento así como las numerosas muestras recogidas para cada usuario en las dos visitas realizadas.

La base de datos necesita ser generada bajo unas condiciones similares para todos los sensores y para todas las comparaciones, ya que se busca la estandarización tanto de los sensores como de la base de datos. Por ello, se generó en el laboratorio donde la temperatura tenía una media de 26 ºC y una humedad relativa del 35 %. Además, el laboratorio cuenta con una buena iluminación proporcionada por fluorescentes situados en el techo.

La base de datos estaba organizada en 50 carpetas, cada una correspondiente a un usuario, dentro de cada carpeta se encontraban todas las imágenes capturadas en las dos visitas, incluido el reclutamiento, de los tres sensores utilizados (Figura 11)

Figura 15: Sensores utilizados, de izquierda a derecha, NXT, FPC y UPK

Que únicamente se utilice una parte de la base de datos es debido al tiempo que la aplicación creada necesita para realizar las comparaciones, siendo de meses el tiempo necesario para poder realizar el procesado de 580 usuarios teniendo en cuenta el análisis de interoperabilidad.

Por último, hasta que el programa no estuvo terminado no se ejecutó en el laboratorio con los 50 usuarios, ya que debido al cumplimiento de la ley de protección de datos, las imágenes de los 50 usuarios debían permanecer siempre allí. Por lo que hasta ese momento la aplicación se iba probando únicamente con alguna de las huellas de dos usuarios, con el fin de cumplir dicha ley de protección de datos de los usuarios participantes en la evaluación. Las primeras huellas eran las pertenecientes a dos usuarios que dieron el consentimiento para el tratamiento de las mismas.

3.3.1 Modificaciones de la base de datos

Con el fin de mejorar el procesado de comparación de las imágenes en la aplicación, la base de datos que se ha utilizado pasó por una serie de filtros, los cuales eliminaban las imágenes que fueron reclutadas con errores en el reclutamiento (FTE).

Todas las imágenes capturadas incluyen el valor de NFIQ, este valor es el que determina la calidad de la imagen. NFIQ tiene una escala del 1 al 5 donde el valor 1 hace referencia a una imagen con buena calidad mientras que el valor 5 hace referencia a una imagen con calidad pésima. Con el fin de utilizar como imagen de reclutamiento, es decir, como patrón, imágenes con una calidad aceptable, fueron eliminadas de la base de datos aquellas imágenes recogidas durante el reclutamiento cuyo valor NFIQ era de 5.

3.4 Proyectos o herramientas de partida

3.4.1 NBIS Biometric Image Software

Se trata de un algoritmo biométrico para la comparación de huellas dactilares. Fue creado por el NIST (National Institute of Standards and Technology), Instituto Nacional de Estándares y Tecnología, de la Oficina Federal de Investigaciones, FBI (Federal Bureau of Investigación) y el departamento de Seguridad Nacional, DHS (Department of Homeland Security).

Este algoritmo no requiere de ningún permiso para su utilización, por lo que se define como una herramienta de dominio público [31].

NBIS se organiza en los siguientes cincos paquetes [32]:

- PCASYS, paquete que permite la clasificación de patrones de huellas digitales según la semejanza con una serie de prototipos de patrones.
- MINDTCT, se trata de un detector de minucias de huellas digitales.
- NFIQ, se trata de un algoritmo que permite determinar la calidad de la imagen.
- AN2K7, se trata de una implementación es de la norma ANSI / NISTITL.
- IMGTOOLS, se trata del conjunto de herramientas necesarias para el procesado de imágenes.

Esta herramienta dispone de una versión desarrollada para .NET, versión utilizada en el proyecto.

Para la creación de la aplicación con la que realizar las comparaciones de huellas dactilares ha sido necesario utilizar una serie de funciones, ya implementadas, proporcionadas por esta herramienta. Para ello se ha incluido la librería NBIS dentro de la aplicación, con el fin de poder acceder a dichas funciones.

La biblioteca NBIS tiene una serie de funciones organizadas en clases, por lo que para acceder a la función es necesario acceder previamente a la clase a la que pertenece.

De las numerosas funciones que tiene implementadas NBIS se han utilizado tres, primero se han combinado dos de ellas con el fin de introducir una imagen de una huella dactilar y conseguir el vector de características, el cual incluye las minucias de la imagen introducida. La tercera se ha utilizado para determinar el resultado de la comparación de las huellas dactilares.

3.4.1.1 Funciones utilizadas

3.4.1.1.1 LoadFileIntoBitmap

Función de la clase “Shared” de NBIS, su funcionamiento es el siguiente:

La función recibe como argumento de entrada la dirección donde se encuentra la imagen de la huella dactilar a comparar, la transforma a un “Bitmap”, es decir, a una imagen binaria, una imagen de ceros y unos, y devuelve dicho “Bitmap”.

3.4.1.1.2 FromBitmap

Función de la clase “DetectMinutiae” de NBIS, cuyo funcionamiento es el siguiente:

La función recibe como parámetros de entrada el “Bitmap” generado en la función “LoadFileIntoBitmap”, con el formato modificado como se explicará en la sección 3.1.3.4, y la resolución vertical del mismo, con el fin de extraer las minucias del “Bitmap” introducido y devolver el vector de dichas minucias.

3.4.1.1.3 Matcher.

Es una función de la clase "Compare" de NBIS que se encarga de comparar dos imágenes con el fin de determinar si se trata de la misma huella dactilar. Recibe dos parámetros de entrada, primero el vector de minucias del patrón que se desea comparar y como segundo parámetro el vector de minucias correspondiente a la imagen de identificación. La función compara los dos vectores de las dos imágenes y determina un valor, denominado resultado de comparación.

Como se ha explicado anteriormente, la igualdad de imágenes se determina por semejanza entre las imágenes a comparar, ya que no se trata de comparaciones binarias. Es por ello que la función "Matcher" tiene una escala de valores para el resultado de comparación, desde 0 a 300, siendo 0 el valor en el cual las imágenes no tienen ningún tipo de semejanza y 300 el valor en el que se trata de la misma imagen.

Como las comparaciones son por probabilidad de semejanza, cuando esta función devuelve un valor cercano al cero estaremos hablando de comparaciones cuyas imágenes no corresponden al mismo usuario, sin embargo, cuando las imágenes corresponden al mismo usuario y al mismo dedo, es decir, las imágenes son de un genuino el resultado de comparación adquirirá valores elevados.

Se da el caso en el que la función "Detectminutiae" no es capaz de sacar ninguna minucia de una imagen, esto puede ser debido a que la imagen capturada no tiene ninguna huella bien definida, es una imagen donde se ha capturado solo una parte de la huella o incluso se trata de una imagen negra. Si se producen estas situaciones (Figura 16) la función "Matcher" recibe un parámetro cuyas minucias son cero por lo que devuelve un cero como resultado de comparación. Es por esto por lo que se pueden encontrar ceros en los ficheros de resultados.

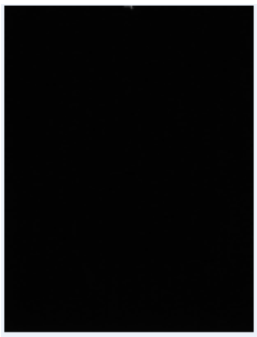


Figura 16: Imagen de una huella dactilar mal capturada.

También se puede dar el caso en el que un resultado de comparación correspondiente a un genuino presente un valor cercano al cero, esto nos indica que las dos imágenes a comparar no guardan semejanza aun correspondiendo al mismo dedo del mismo usuario. Esta situación es debida a que alguna de las dos imágenes, y raramente las dos, no se tomó de manera correcta. El caso más común es que el usuario retirase el dedo antes de que se produjese la captura o se rotase el dedo mientras esta se estaba realizando (Figura 17), lo que da lugar a una imagen borrosa, de la cual se puede determinar un número reducido de minucias.

En esta situación el vector de minucias de esta imagen guardará escasa semejanza a los demás vectores de minucias correspondientes a imágenes del mismo dedo dando lugar a errores de falso rechazo y provocando el incremento de las tasas FNMR y/o FRR

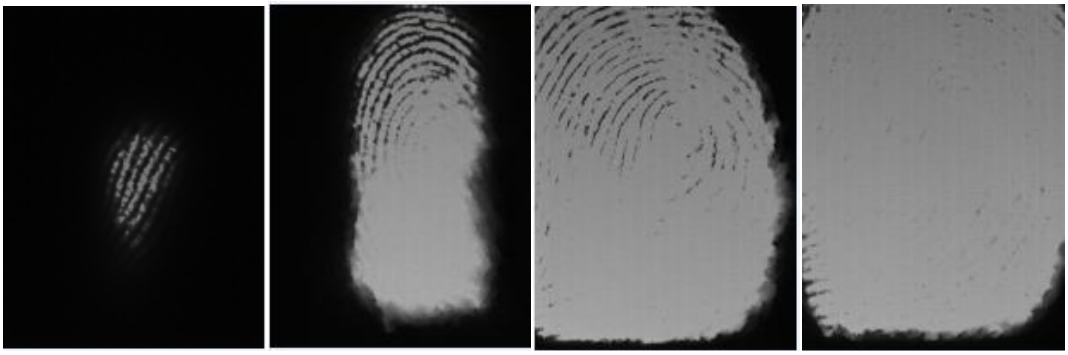


Figura 17: Ejemplos de huellas dactilares con defectos en las capturas.

El caso contrario, es decir, que el resultado de dos imágenes correspondientes a impostores presente un resultado de comparación elevado se da en un porcentaje menor, ya que un error de captura es más difícil que cree un vector de minucias semejante al vector de minucias de la imagen a comparar. Pero cuando ocurre, el resultado de la comparación es elevado, incrementándose el numero de errores de falsa aceptación y por lo tanto las tasas FMR y/o FAR.

3.4.2 Biosecure Tool

Se trata de una herramienta biométrica que contiene un conjunto de funciones implementadas en Matlab cuya función principal es EER_DET. Esta función proporciona una serie de datos reflejados en curvas y valores con el fin de realizar análisis biométricos, tales como la evaluación del rendimiento de un sistema de reconocimiento biométrico.

3.4.2.1 Parámetros de entrada de la función EER_DET

La función recibe como parámetros de entrada, los siguientes datos:

- "Clients": Vector de los resultados de comparación de genuinos, entendiendo por genuino aquella comparación en la que las huellas a comparar pertenecen al mismo dedo de un mismo usuario.

- "Impostors": Vector de los resultados de comparación de impostores, se habla de impostores cuando las huellas a comparar pertenecen a usuarios diferentes.

- α: este valor es él valor de la tasa de FAR (porcentaje de falsa aceptación) para el que se desea obtener el valor de la tasa FRR, dada la dependencia entre ambas tasas. El valor recomendado es de 0.01.

- N: número de iteraciones para calcular las curvas o distribuciones de puntuación. Se aconseja un valor de 100 iteraciones.

3.4.2.2 Parámetros de salida de la función EER_DET

Gracias a esta herramienta se obtienen los siguientes cuatro parámetros de salida:

- Curva ROC (Receiver Operating Characteristic)

  Se trata de una curva independiente del valor del umbral de decisión, lo que permite medir y comparar el rendimiento de los diferentes sistemas en condiciones similares.

  Esta curva se obtiene representando en el eje X el porcentaje de intentos para los que ha sido aceptada una imagen de un impostor, es decir, la tasa de falsa aceptación FAR. Mientras que en el eje Y se representa el porcentaje de intentos de auténticos usuarios genuinos, es decir, 1 – tasa de falso rechazo, 1-FRR.

- Curva DET

  La curva DET proporciona la misma información que la curva ROC pero expresada de manera diferente, ya que en esta curva se representa en el eje X la tasa de falsa aceptación FAR frente a la tasa de falso rechazo FRR que se representa en el eje Y

- Punto del EER

  Es el punto donde el valor de la tasa de falsa aceptación FAR se iguala al valor de la tasa de falso rechazo FRR.

- Punto operación OP

  Es el punto que representa el valor de la tasa de falso rechazo FRR para un determinado valor de la tasa de falsa aceptación FAR, en este caso definido por el valor α.

3.5 Plataformas de desarrollo

3.5.1 Visual Studio

Se trata de un conjunto de herramientas de desarrollo para la creación de múltiples aplicaciones, tales como, aplicaciones web, servicios web, aplicaciones móviles, etc [33].

Esta herramienta soporta múltiples lenguajes de programación como: C++, C#, Visual Basic .NET, F#, Java,Python, Ruby, PHP [34].

Visual Studio permite crear soluciones en varios lenguajes de programación, esto es debido a que la mayoría de ellos utilizan el mismo entorno de desarrollo integrado, IDE, del inglés Integrated Development Environment. El IDE facilita la creación de las aplicaciones ya que contiene herramientas de ayuda para diseñar, escribir, editar y depurar el código de la aplicación [35].

Esta herramienta está disponible en numerosas versiones, cada una con mejoras con respecto a la versión anterior, para el desarrollo de la aplicación necesaria se utilizó Visual Studio 2013, la actualización más reciente.

3.5.1.1 Lenguaje de programación utilizado

De las múltiples posibilidades de lenguaje de programación que ofrece Visual Studio, para la creación de la aplicación de comparación de huellas dactilares se ha utilizado el lenguaje C#.

Se trata de una variante del lenguaje de programación C. Tanto C como C++, otra de las variantes del primero, ya fueron utilizadas a lo largo del grado universitario en las asignaturas que requerían de un lenguaje de programación, asignaturas informáticas, lo que hace que se tengan ciertos conocimientos acerca de este lenguaje y sus variantes. Es por ello que se llegó a la elección de este lenguaje entre todos los disponibles, ya que cualquier problema con el código sería más fácil de detectar y entender si se había trabajado previamente con el lenguaje utilizado.

C#, al igual que C, es un lenguaje orientado a objetos, se trata de un lenguaje simple, eficaz, con gran documentación de uso y proporciona gran seguridad.

3.5.2 Matlab

Se trata de una herramienta de software matemático, que proporciona un entorno de desarrollo integrado (IDE), a diferencia de Visual Studio, ésta posee un lenguaje de programación propio, lenguaje M [36].

Matlab posee múltiples prestaciones, entre las que destacan: la manipulación de matrices, la representación de datos y funciones, la implementación de algoritmos, etc.

Es una herramienta destinada a proyectos donde se necesite un número elevado de cálculos matemáticos y la representación grafica de los mismos. Por último, decir que se trata de una herramienta con gran documentación de uso lo que simplifica tanto el seguimiento y comprensión de soluciones ya implementadas como el diseño y desarrollo de nuevas soluciones.

4. IMPLEMENTACIÓN DE LA SOLUCIÓN

Para la realización de cualquier proyecto es recomendable realizar una estructura previa del trabajo, con el fin de optimizar el tiempo empleado en la realización del mismo y conseguir los mejores resultados.

Esta idea se acentúa cuando se trata de un proyecto donde es necesaria la programación, dado que sin un estudio previo de los datos necesarios y de la implementación para la obtención de los resultados, la programación puede resultar complicada y se puede llegar a obtener resultados erróneos, lo que supondría la necesidad de más tiempo para desarrollar la solución. Es por ello que es de vital importancia una buena estructura donde se incluya una organización previa de las diferentes posibilidades, con el fin de elegir el camino que proporcione de manera más eficiente los datos necesarios para el posterior análisis.

Se ofrece un diagrama de bloques Figura 18 del proceso general del proyecto.

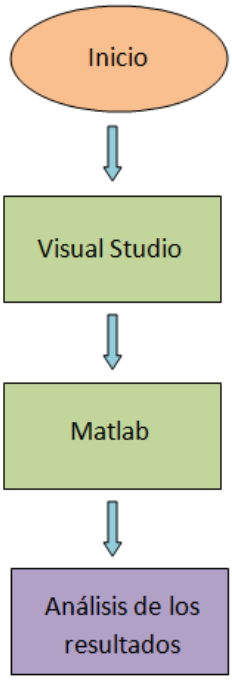


Figura 18: Diagrama de bloques general del proyecto.

4.1 Aplicación en Visual Studio

4.1.1 Planteamiento inicial

Antes de comenzar a implementar la aplicación, se estudió qué resultados se buscaban obtener y cuál de los diferentes caminos era el que más se adaptaba a lo que se necesitaba. Para ello se creó una estructura inicial del proyecto, aunque, según se iba desarrollando la solución iban surgiendo nuevas ideas que hacían necesario reorganizar la estructura inicial con el fin de mejorar el proyecto.

La base del proyecto era crear una aplicación automática para la comparación de huellas dactilares, con el fin de obtener los resultados de las comparaciones para posteriormente realizar análisis de rendimiento estudiando la interoperabilidad de los sensores utilizados.

La metodología de trabajo utilizada fue comenzar por la creación de una aplicación sencilla que cumpliera con los requisitos esperados, por ello se comenzó por crear una aplicación cuyo funcionamiento era manual, ya que con una aplicación automática es más complicado detectar los fallos y conseguir que la aplicación realice lo esperado.

Tras la implementación de esta aplicación sencilla, aplicación de consola, se traspasó el código a una aplicación más compleja, y se realizaron las adaptaciones necesarias a la nueva aplicación, aplicación WPF, ésta siguió siendo manual hasta que la aplicación funcionaba correctamente.

Una vez el programa estaba terminado de manera manual la restructuración más importante que se realizó fue el cambio del método manual para pasar a la implementación de la automatización absoluta de la aplicación.

4.1.2 Aplicación de consola.

Dentro de la plataforma Visual Studio se pueden crear diferentes aplicaciones, con diferentes grados de dificultad.

En base a la idea de comenzar por una aplicación sencilla para, una vez que se obtengan los resultados esperados, pasar a implementar una aplicación con un grado mayor de complejidad la aplicación de comparación se creó previamente en una aplicación de consola con el fin de sentar las bases de la aplicación a implementar.

Cuando hablamos de aplicación de consola nos referimos a una aplicación que se ejecuta en la línea de comandos del ordenador, también llamada ventana de comandos (Figura 19).

Este tipo de aplicaciones utiliza un formato de entrada y salida de datos en modo texto. Únicamente se basa en una clase, la clase “console”, la cual permite mostrar información, así como, capturar la información introducida por el usuario.

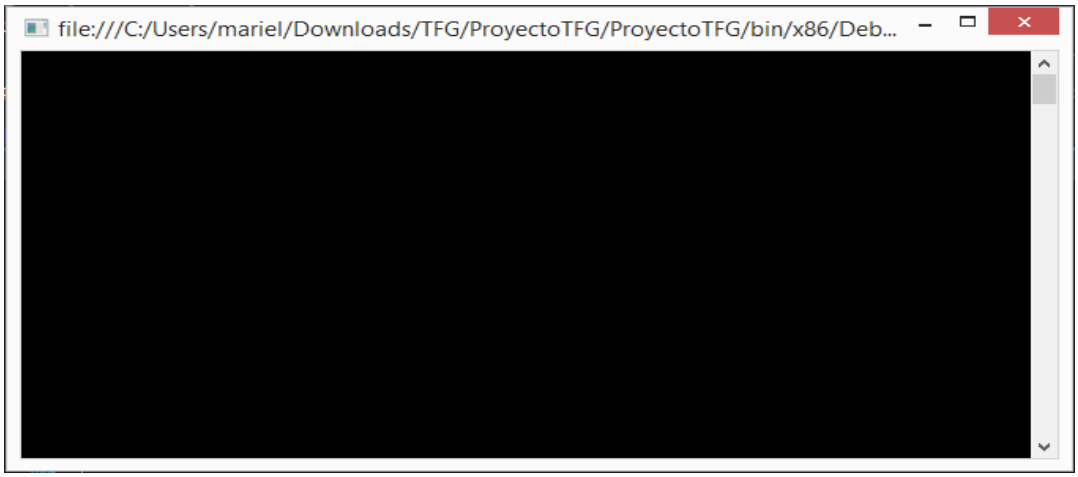


Figura 19: Ventana de comandos.

El funcionamiento manual de esta aplicación es el siguiente:

Lo primero es elegir que dos imágenes se van a comparar, para ello se muestra en la línea de comandos, mediante el método de escritura "WriteLine" de la clase "console", el directorio de las diferentes carpetas disponibles, todas ellas numeradas. Los directorios de dichas carpetas son proporcionados por el método "GetDirectories", este recibe como parámetro de entrada el directorio de la carpeta donde se encuentran las carpetas a mostrar y devuelve el directorio de cada carpeta.

Una vez se introduce el número de carpeta para la primera muestra, el método "GetFiles" proporciona el directorio de los archivos, de las imágenes que se encuentran en la carpeta seleccionada, recibiendo como parámetro el directorio de la carpeta seleccionada. De la misma manera que se nombraba el directorio de las carpetas se muestra el directorio de las imágenes por la línea de comandos mediante el método de escritura "WriteLine", y del mismo modo se introducía por teclado el número de la imagen deseada. Una vez teníamos la primera imagen se volvían a mostrar todas las carpetas para, del mismo modo que para la primera imagen, elegir la segunda.

En esta primera aplicación la selección de imágenes no tenía en cuenta la separación por sensores, por lo que se compraban las imágenes sin importar con que sensor habían sido capturadas.

Cuando se tienen las dos imágenes seleccionadas se procede a la extracción de minucias, a la obtención del resultado de comparación y al almacenamiento de dicho resultado en el fichero correspondiente, procesos que se explicarán detalladamente en la sección 4.1.3.2, ya que una vez seleccionadas las dos imágenes el proceso es muy semejante tanto para aplicación de consola como para WPF manual y automática, por lo que estos procesos se explicarán para la aplicación final, WPF automática.

En una aplicación de consola se van mostrando mensajes por la línea de comandos, como por ejemplo, el directorio seleccionado para cada muestra, el valor del resultado de comparación, o el nombre del fichero donde se almacena cada resultado. Todos estos mensajes se muestran mediante el método "WriteLine", con el fin de realizar un seguimiento detallado del recorrido del programa, y así poder detectar en qué momento se está produciendo algún fallo.

La última línea del código llama al método "ReadLine" de la clase "console", este método evita que al terminar de ejecutar el programa la ventana de la línea de comandos se cierre e imposibilite la lectura de los mensajes.

En la Figura 20 se muestra la ventana de comandos con el proceso manual de la comparación de dos huellas dactilares, con los correspondientes mensajes para el seguimiento del proceso.

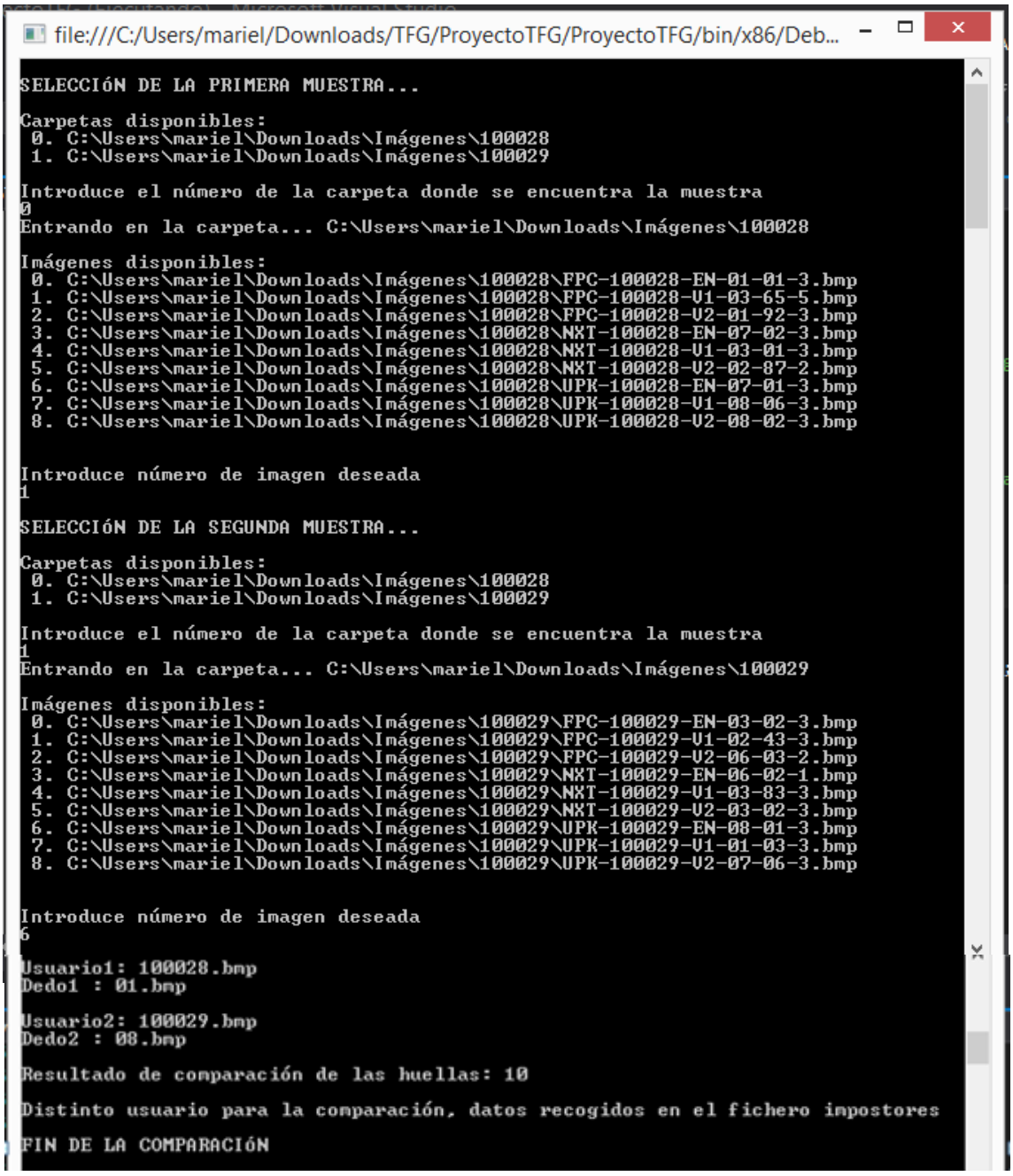


Figura 20: Funcionamiento de la aplicación de consola.

4.1.3 Aplicación WPF

Una vez la aplicación de consola funcionaba correctamente, es decir, se controlaba la selección de imágenes, los resultados eran los esperados y cada resultado se guardaba en el fichero correspondiente se procedió a la creación de la aplicación WPF.

A diferencia de las aplicaciones de consola, las WPF no utilizan la línea de comandos para la entrada o salida de datos, sino que utilizan ventanas donde las entradas se realizan a través de la activación o desactivación de botones y las salidas mediante textos incluidos en ventanas, de menor tamaño, con opciones como aceptar o cancelar.

Este tipo de aplicacion permite obtener aplicaciones más llamativas e intuitivas, ya que la creación de ventanas y la utilización de botones vistosos proporcionan un correcto guiado y entendimiento de la actividad o del programa.

En el estudio previo de esta aplicación se estudió que información se incluiría en la pantalla principal así como los tipos de botones necesarios para las pruebas a realizar. Además, se pensó en la información que se daría en cada pantalla de la aplicación en modo manual.

La ventana principal de la aplicación es la misma tanto si la selección es manual como si es automática, esta ventana se puede apreciar en la Figura 21:

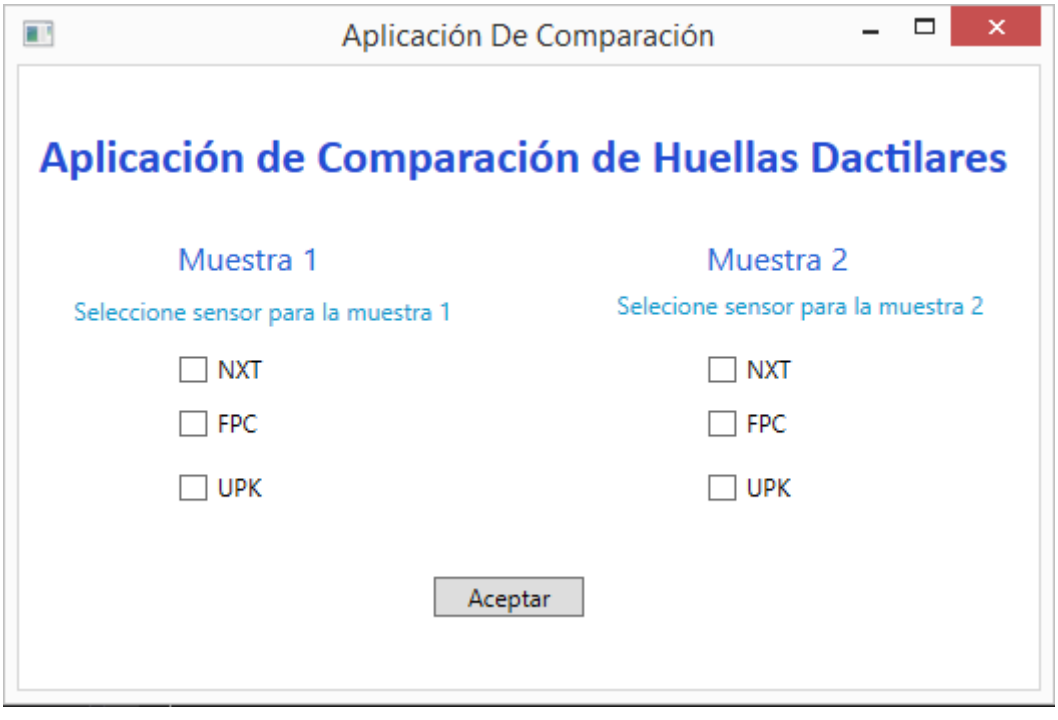


Figura 21: Ventana principal de la WPF.

Como se aprecia en la Figura 21 encontramos seis botones "checkbox", tres de ellos situados en la parte derecha con el nombre de los tres sensores disponibles para la muestra 1, imágenes de reclutamiento, y otros tres situados en la parte izquierda, que del mismo modo contienen el nombre de los tres sensores disponibles para la muestra 2, imágenes de muestras de usuarios proporcionadas en las diferentes visitas para el reconocimiento.

Los botones "checkbox" son casillas de verificación por accionamiento de un botón, que especifica dos estados, activado o desactivado. Todos ellos están numerados con el fin de diferenciarlos a la hora de utilizarlos en la programación del código. Se han elegido este tipo de botones ya que permiten la activación de varios a la vez. Los "checkbox" se utilizan para seleccionar qué sensor se desea utilizar como sensor para la fase de reclutamiento y qué sensor se va a utilizar como sensor para la fase de reconocimiento.

Por otro lado la ventana principal cuenta con un "Button" con el nombre de "Aceptar", que se encarga de dar comienzo a la aplicación, por lo que cuando se activa el botón "Aceptar" da comienzo la ejecución del programa.

4.1.3.1 Aplicación WPF manual

El modo manual de esta aplicación únicamente se diferencia del modo automático en la manera de seleccionar las imágenes, por lo que en este apartado únicamente se mostrará cómo se eligen las imágenes en una WPF manualmente, los siguientes procesos, al ser los mismos que en el modo automático se expondrán en ese apartado. La única diferencia serán los mensajes de seguimiento de la aplicación manual, los cuales pueden ser suprimidos para el modo automático dado que únicamente sirven de guía en el seguimiento del programa y la detección de errores.

El método utilizado para la selección de imágenes en la WPF es el método "OpenFileDialog()", éste abre una ventana como la que se muestra en la Figura 22, donde se permite seleccionar la imagen elegida para la comparación.

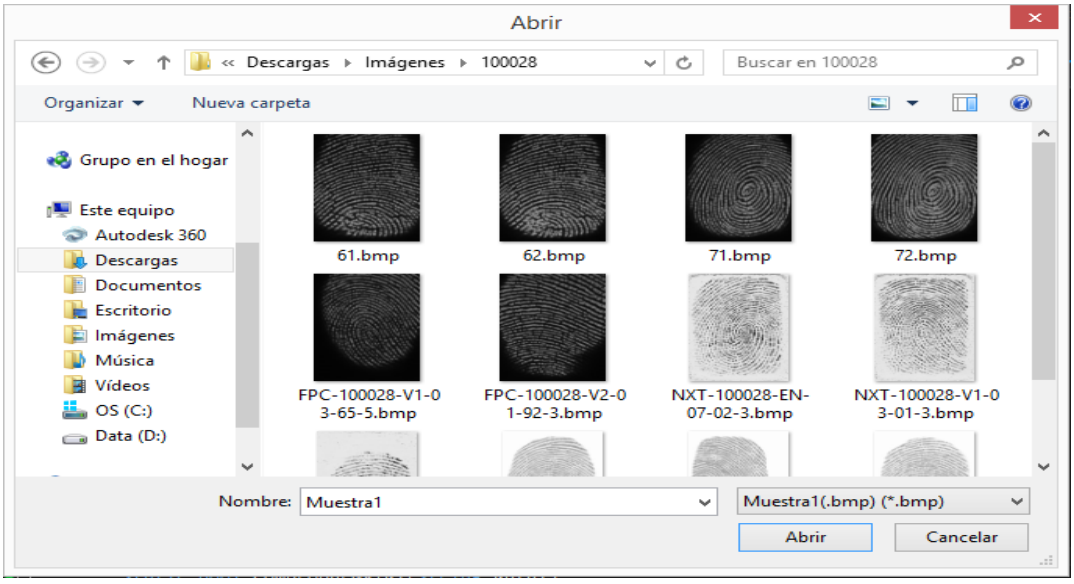


Figura 22: Ventana para la selección manual de imágenes.

A diferencia de la aplicación de consola ésta tiene en cuenta el sensor con el que se capturó la imagen, por ello, si en la ventana principal se marcó el "checkbox" de un sensor y, al seleccionar la imagen el nombre del sensor con el que está capturada no coincide con el nombre del "checkbox" activado, la aplicación devuelve un mensaje de error (Figura 23) y da la posibilidad de volver a seleccionar la imagen. De la misma manera ocurre con las imágenes de la muestra 2, imágenes de las visitas.

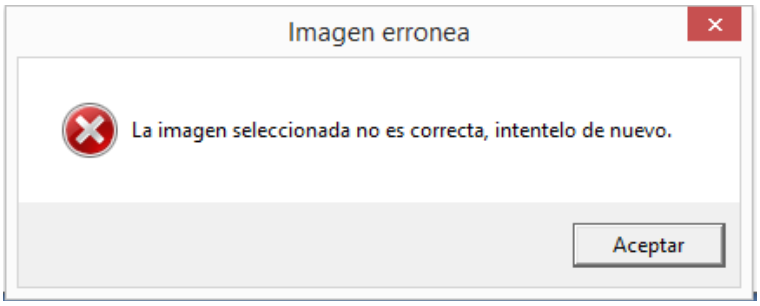


Figura 23: Error en la selección del sensor de captura.

Al igual que en la aplicación de consola, era necesario seguir el proceso de comparación con el fin de resolver eficazmente los errores cometidos en la implementación, por ello, mientras la aplicación era manual se iba mostrando el recorrido del proceso mediante ventanas con la opción de aceptar (Figura 24).

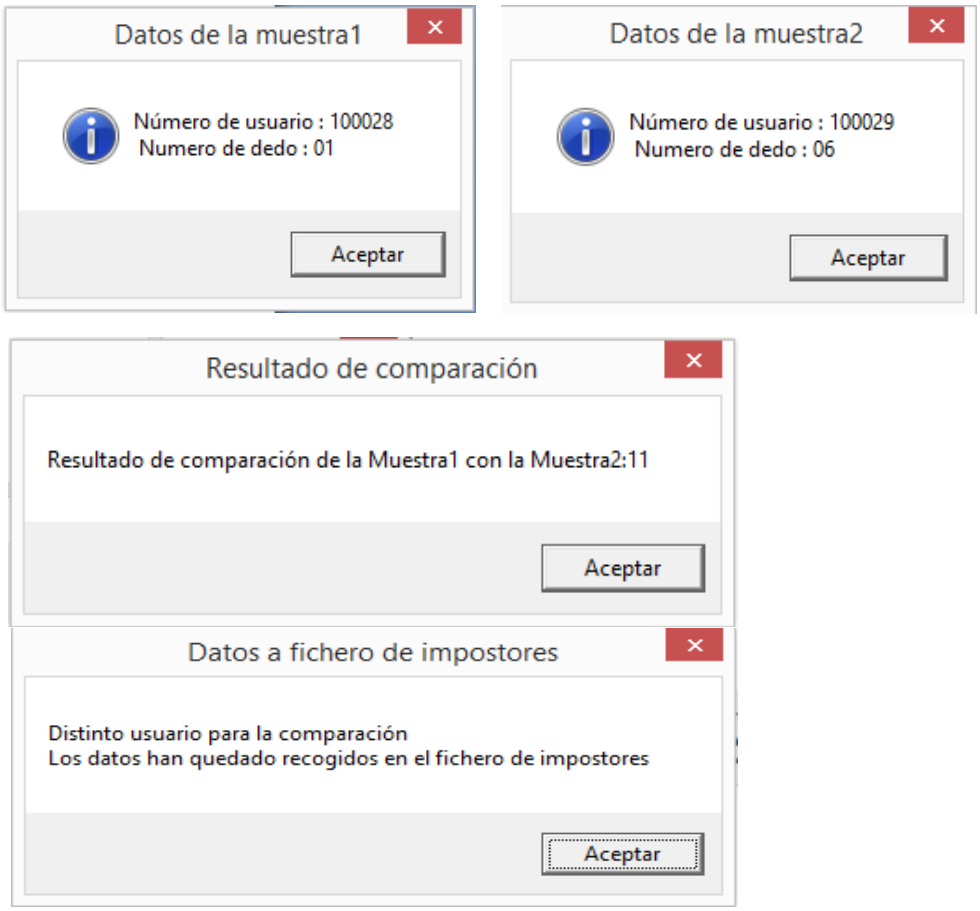


Figura 24: Mensajes de seguimiento de la WPF manual.

Una vez que la WPF manual funcionaba correctamente se pasó a automatizar la aplicación, haciendo que el proceso de selección de las imágenes se realice por sí solo en función de los sensores marcados en la ventana principal. Asimismo se suprimieron los mensajes intermedios que estaban destinados a conocer los pasos intermedios que se iban realizando.

4.1.3.2 Aplicación final: WPF automática.

La aplicación final cumple con el objetivo inicial del proyecto, obtener los resultados de comparación de las imágenes de una base de datos, de forma que la única interacción que se necesite sea la selección de los sensores cuyas imágenes se desean comparar. A continuación, se ofrece un esquema (Figura 25) del funcionamiento de la aplicación.

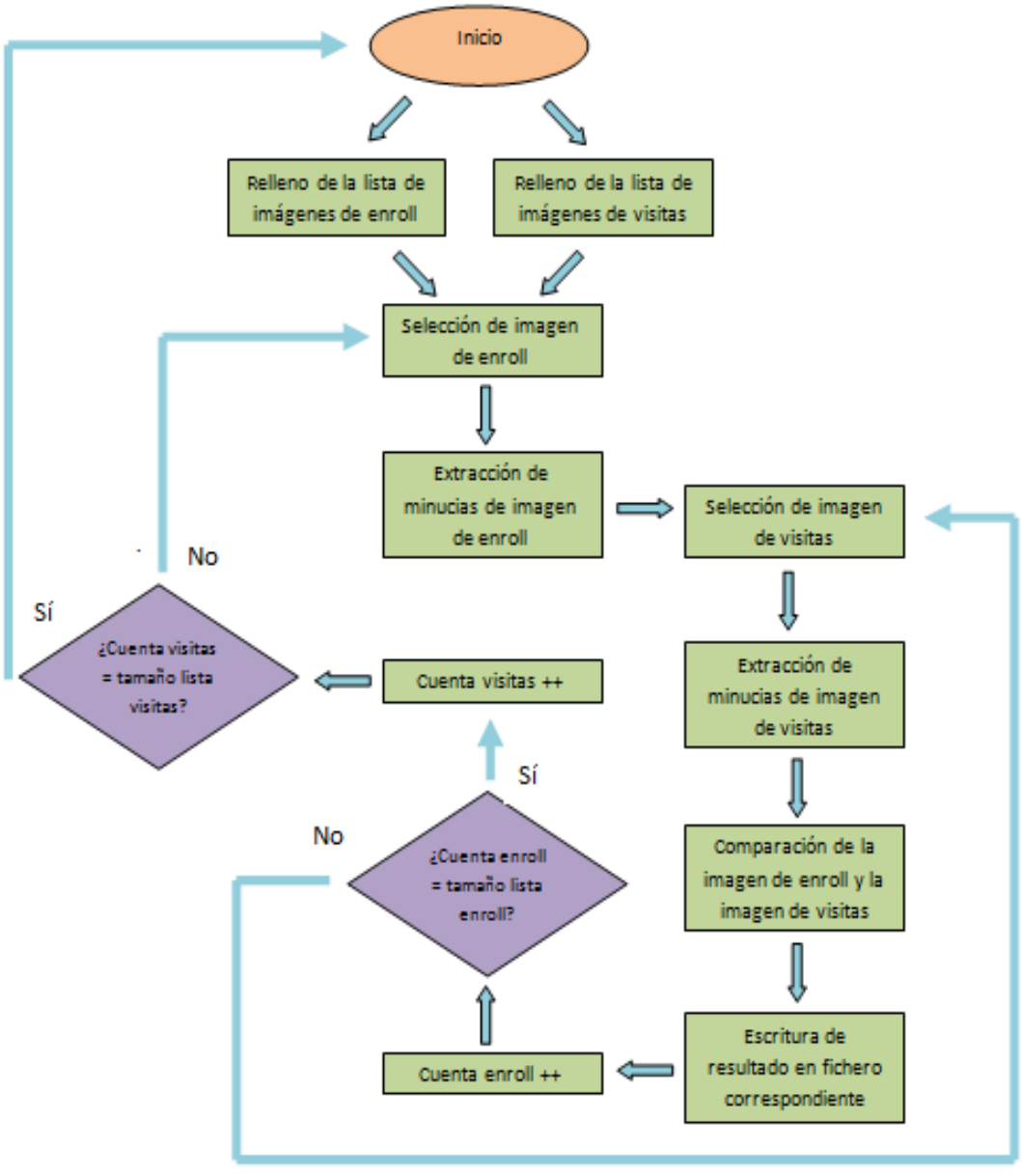


Figura 25: Diagrama de bloques de la aplicación en Visual Studio.

Una vez se procede a la ejecución del programa aparece la ventana principal de la aplicación, ésta se muestra en la Figura 21. En ella se puede seleccionar, para la muestra 1, el sensor que se desea utilizar como sensor de reclutamiento. A continuación, en esta misma pantalla, se permite elegir el sensor que se desea utilizar como sensor para el reconocimiento, muestra 2. Ambas selecciones se validan activando el botón "Aceptar".

Una vez activado este botón, se inicia el programa, cuyo funcionamiento es el siguiente:

Al validar la selección, el programa evalúa cuál de los "checkbox" está activado y, según esta decisión se adjudica el nombre del sensor cuyo "checkbox" este activado para la muestra 1 a una variable de tipo "string", denominada "Sensor1", y el nombre del sensor activado para la muestra 2 a otra variable, también de tipo "string", denominada "Sensor2". El término "string" es un término informático que hace referencia a una secuencia de ceros o más caracteres.

Primero se crean dos listas de "strings", una de ellas contiene todas las imágenes de reclutamiento, de todos los usuarios, que contengan el nombre adjudicado a la variable "Sensor1"; mientras la otra está formada por la concatenación de todas las imágenes de reconocimiento capturadas durante la visita 1 y la visita 2, también de todos los usuarios, que contengan el nombre adjudicado a la variable "Sensor2".

En esta primera parte también se crean cuatro ficheros, dos de ellos van destinados a guardar los datos de los resultados de las comparaciones de genuinos e impostores. Estos ficheros se nombran en función de los valores que tengan las variables "Sensor1" y "Sensor2".En cuanto a los otros dos, son ficheros contadores y su misión es a llevar la cuenta de las imágenes procesadas de reclutamiento y de reconocimiento en cada momento.

Los ficheros de genuinos e impostores son distintos para cada una de las nueve pruebas que se van a realizar en el estudio ya que son nombrados al iniciar cada una de las pruebas, en base al nombre de los sensores elegidos en la ventana principal atendiendo a la siguiente estructura:

FicheroGenuinosSensor1-Sensor2 y FicheroImpostoresSensor1-Sensor2.

Según esta estructura para la primera prueba, donde el sensor de reclutamiento es NXT y el sensor de reconocimiento es NXT el nombre de los ficheros quedaría de la siguiente manera (Figura 26):

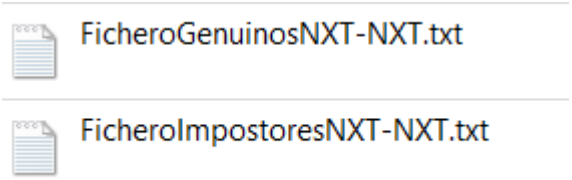


Figura 26: Ejemplo de ficheros para la prueba NXTNXT.

El nombrar los ficheros de esta manera se realizó con el fin de diferenciarlos a la hora de procesarlos en Matlab, es por ello que cuando se termina una prueba y se va a realizar la siguiente se crean dos ficheros nuevos, con los nombres de los sensores activados en la nueva prueba.

Los dos últimos ficheros creados, es decir, los ficheros destinados a llevar la cuenta de las imágenes procesadas para el reclutamiento y las imágenes procesadas para el reconocimiento se generan para poder reanudar las pruebas de comparación en caso de que exista algún tipo de error durante la ejecución de la aplicación por el problema de memoria del programa, ya que cuando el programa procesa un número determinado de usuarios salta una excepción de memoria insuficiente, por lo que el programa se para y es necesario volverlo a iniciar, con el fin de no perder los datos procesados en ningún momento. En particular en estos dos ficheros se guarda la posición de cada una de las listas de forma que cuando se produce una excepción y se vuelve a iniciar el programa éste lee el valor de los dos ficheros que llevan la cuenta de la posición donde se quedó el programa y continúa las comparaciones desde ese punto.

A diferencia de los ficheros destinados a guardar los resultados de genuinos e impostores, los ficheros contadores son los mismos para las nueve pruebas (Figura 27) ya que solo sirven para ejecutar la comparación completa de una prueba, por lo que una vez terminada una prueba se elimina el valor que tuviesen los ficheros y se inicializa a cero para comenzar con la siguiente prueba.

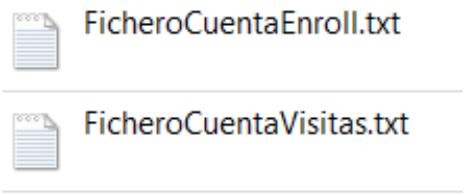


Figura 27: Ficheros contadores.

La aplicación creada se basa en obtener los resultados de comparación de todas las imágenes de reclutamiento frente a todas las imágenes de reconocimiento, para ello se van recorriendo automáticamente la lista que contiene las imágenes de reclutamiento correspondientes al nombre del sensor activado y la lista que contiene las imágenes de reconocimiento del sensor seleccionado, comparando sus resultados de la siguiente manera:

Se crean dos bucles “for”, el primero para recorrer la lista de las imágenes de reclutamiento, desde el valor del fichero que lleva la cuenta de las imágenes de reclutamiento procesadas (en caso del comienzo de una prueba el fichero tendrá un cero), hasta el tamaño de la lista de todas las imágenes reclutamiento. El segundo bucle “for” se encuentra dentro del primero para recorrer las imágenes de reconocimiento, de la misma manera, desde el valor que tenga el fichero de la cuenta de las imágenes de reconocimiento procesadas hasta el tamaño de dicha lista (del mismo modo, si se inicia una prueba, el valor del fichero será cero).

Al entrar el programa en el primer bucle se selecciona de manera automática un único reclutamiento para cada uno de los dedos de cada usuario, con el fin de no repetir comparaciones. Es por ello que si el programa detecta que para un usuario y un dedo el sistema ya ha comparado una imagen de reclutamiento, la ignora y pasa a la siguiente. Este proceso se repite para la selección de todas las imágenes de reclutamiento. El proceso en concreto sería el siguiente. Una vez que se ha seleccionado la primera imagen de reclutamiento del primer usuario ésta se convierte a un mapa de bits mediante la función "LoadIntoBitmap". Además se produce la extracción de minucias mediante la función "FromBitmap" y se extrae el número de usuario y de dedo reflejado en el directorio de la foto. Esto último se realiza mediante la combinación de funciones destinadas a trabajar con variables de tipo "string".

En este punto comienza el segundo bucle, que selecciona la primera imagen de reconocimiento y obtiene sus minucias, así como el usuario y dedo al que pertenece la foto, de la misma manera que se realizó para la imagen de reclutamiento. Una vez se tienen las minucias de las dos imágenes a comparar se pasan a la función "Matcher" la cual al introducir dos vectores de minucias los compara y proporciona un resultado de comparación.

Llegados a este punto entramos en dos secuencias "if", si las imágenes comparadas se corresponden al mismo dedo del mismo usuario el resultado de la comparación se escribirá en el fichero de genuinos, pero, si el usuario de las dos muestras no es el mismo, el resultado de comparación pasará a escribirse en el fichero de impostores, este proceso se muestra en la Figura 28. Ambas opciones incrementarán la cuenta del fichero de imágenes de reconocimiento. Este segundo proceso se realizará con todas las imágenes de visitas. Una vez el segundo bucle realice la comparación de la última de las imágenes de reconocimiento, se terminará por el momento el segundo bucle para pasar a la siguiente posición del bucle de imágenes de reclutamiento, incrementando a su vez la cuenta del fichero de reclutamiento. A partir de aquí se realizará de nuevo el procedimiento comentado para las siguientes imágenes de reclutamiento y reconocimiento.

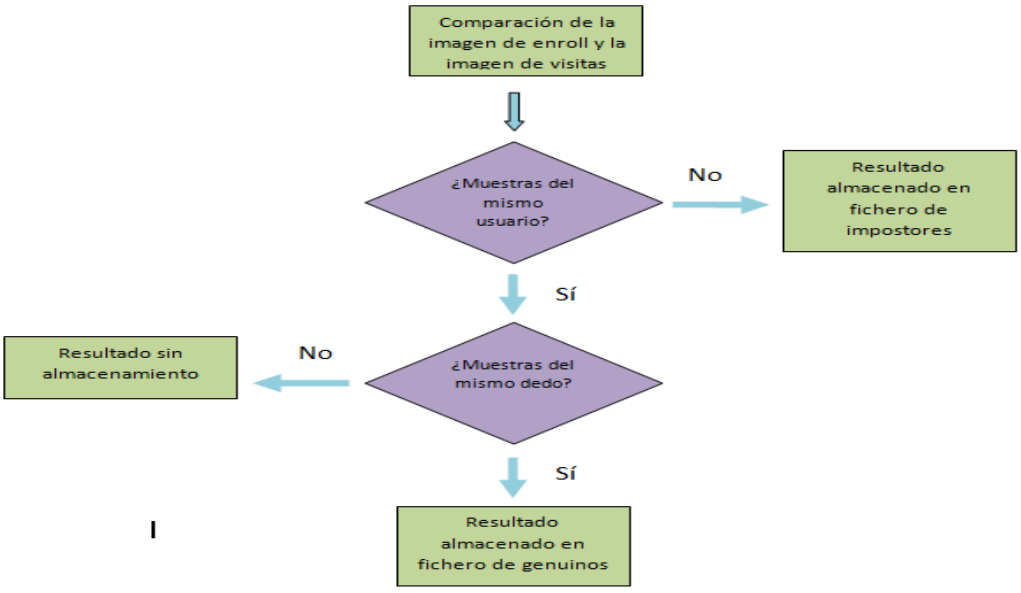


Figura 28: Diagrama de bloques detallado del almacenamiento de los resultados.

En el momento en el que el programa se detenga debido a cualquier tipo de error, lo primero que hará el programa al volver a iniciar la aplicación será leer el valor que contengan los dos ficheros, valor que corresponde con la posición de las listas de la última comparación que realizó el programa antes de su parada, por lo que comenzará las comparaciones desde esas posiciones.

4.1.3.3 Gestión de la memoria de la aplicación.

Como se ha comentado en el aparatado 4.1.3.1, cuando la aplicación procesa un determinado número de usuarios aparece una excepción de memoria insuficiente. Esta excepción se trató de solucionar incluyendo métodos y funciones destinados a eliminar los objetos innecesarios.

4.1.3.3.1 Método Dispose()

Método que poseen los objetos de algunas clases, como por ejemplo la clase "Bitmap", para liberar la memoria de los objetos que ya no va a ser utilizados.

Una vez que el "Bitmap" deja de ser utilizado el objeto llama a este método y éste se encarga de liberar la memoria correspondiente a dicho objeto. La liberación de memoria por parte de éste método es inmediata y no requiere de gran cantidad de tiempo para realizar la acción.

Este método fue utilizado con éxito para liberar, tras la comparación de cada imagen los objetos "Bitmap" utilizados así como los objetos de la clase "ImageToMatrix" y de la clase "MatrixToBitmap" necesarios en el proceso de transformación del formato de los "Bitmap".

4.1.3.3.2 Garbage Collect()

Se trata de una función encargada de liberar la memoria correspondiente a todos los objetos que no van a volver a ser utilizados. Esta liberación de memoria se produce cuando el programa determina que debe realizarse dicha acción, lo que hace imposible conocer el momento en el que se va a producir la liberación.

Con el fin de forzar la liberación de la memoria se utiliza la función "WaitForPendingFinalizers()". La llamada a esta función se realiza inmediatamente después de la llamada a la función "Collect()" y su misión es detener el programa hasta que el "Garbage Collect" libere toda la memoria disponible.

La llamada a estas funciones se puede realizar varias veces en cualquier momento de la ejecución del programa, sin embargo, estas funciones requieren de gran tiempo de ejecución, por lo que se debe considerar el número de veces que se van a utilizar con el fin de no invertir tiempo innecesario en liberar memoria.

A diferencia del método "Dispose()", estas dos funciones no fueron capaces de eliminar los objetos innecesarios con éxito, lo que provocaba errores de memoria insuficiente periódicamente. Este problema se solucionó mediante la creación de los dos ficheros encargados de guardar la última comparación realizada antes de la parada del programa, con el fin de comenzar en ese punto cuando se reanudaba la ejecución.

4.1.3.4 Transformación de las imágenes.

El "Bitmap" generado en la función "LoadIntoFile" posee un formato de 32bpp, incompatible con el formato de 8bpp que acepta la función "FromBitmap", por lo que antes de utilizar esta función es necesario modificar dicho formato.

4.1.3.4.1 Método Clone()

Los objetos de la clase "Bitmap" poseen el método "Clone()", el cual permite clonar objetos, por lo que inicialmente, se intentó transformar el "Bitmap" mediante la creación de un rectángulo de 8bpp y la clonación de cada "Bitmap" en dicho rectángulo.

Este método recibe dos parámetros: el primero es la imagen que se va a clonar introducida en el nuevo rectángulo, y el segundo es el formato que se desea conseguir, en nuestro caso 8bpp. A su vez, a la hora de crear el nuevo rectángulo, es necesario indicar cuatro parámetros. Estos cuatro parámetros son: la posición X e Y donde se va a crear el rectángulo, en nuestro caso (0,0), y el tamaño de la imagen a transformar, "Width" y "Height".

Con este método se detectaron errores en la extracción de minucias, ya que todos los vectores tenían un número de minucias cercano a cero. Cuando se procedió a guardar la nueva imagen, mediante el método "Save", de la clase "Bitmap", se detectó que al realizar el cambio de formato la imagen obtenida era la siguiente (Figura 29).

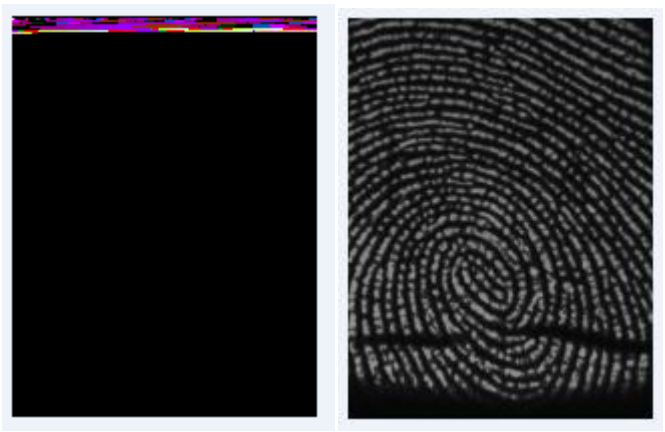


Figura 29: Transformación de Bitmap mediante el método Clone ().

Como se aprecia en la Figura 29 la transformación de la imagen no se realiza de manera correcta, por lo que este método resulto fallido.

4.1.3.4.2 Método Convert()

Tras detectar el fallo del método "Clone()" se procedió a utilizar otro método para la transformación. Para ello se incluyó en el proyecto la biblioteca "Accord" y se utilizó su función "Convert()" para el cambio de formato de imágenes, cuyo funcionamiento es el siguiente:

Se crea un objeto de la clase "ImageToMatrix" el cual llama a la función "Convert()" de la biblioteca "Accord", ésta recibe dos parámetros, en primer lugar recibe el nombre del "Bitmap" a transformar, y en segundo lugar el nombre de la matriz a la que va a ser transformado.

"Convert()" transforma el Bitmap original a una matriz con un rango de 256 posiciones, 8 bpp. Acto seguido se crea un objeto de la clase "MatrixToImage", del mismo modo este objeto llama a la función "Convert()", pero en este caso la función recibe la matriz en la que se transformó el "Bitmap" original y el nombre del "Bitmap" donde se va a transformar la matriz. En esta caso la función "Convert()" transforma la matriz con rango de 8 bpp a un "Bitmap", por lo que el formato del "Bitmap" transformado es de 8bpp.

Con el fin de no repetir código, para este proceso se creó una función la cual recibe como parámetro el "Bitmap" a transformar y devuelve el "Bitmap" transformado.

Tras la implementación de esta parte se comprobó que la imagen que se extraía tras el proceso de cambio de formato era la misma que la original, con el fin de no cometer el error anterior. Como se aprecia en la Figura 30 ambas imágenes son idénticas.

Figura 30. Transformación de "Bitmap" mediante el cambio a matriz.

4.2 Aplicación en Matlab

Una vez se generan los ficheros de genuinos e impostores correspondientes a los resultados de comparación de cada una de las pruebas realizadas con la aplicación creada en Visual Studio, se procede a la utilización de la herramienta "Biosecure Tool" mediante el programa Matlab.

Como se comentó en el apartado 3.4.2.1 esta herramienta necesita de unos parámetros de entrada. En cada una de las nueve pruebas el parámetro "clientes" será un vector que contendrá los valores de las comparaciones de genuinos y se obtiene a partir de la lectura de los datos del fichero de genuinos. Por otro lado, el parámetro "impostors", se corresponderá al vector que contendrá los resultados de las comparaciones de impostores. Asimismo, los valores de α y n son constantes para las nueve pruebas y serán los valores recomendados por la herramienta

Una vez introducidos todos los parámetros de entrada necesarios en la función EER_DET se produce la llamada de dicha función desde la ventana de comandos de "Matlab", para obtener las curvas y valores comentados en el apartado 3.4.2.2

La función EER_DET incluye la función "Plot", que se encarga de la generación de las gráficas. Es por ello que dicha función ha sido adaptada al estudio realizado en este TFG, modificando el conjunto de curvas que se deseasen obtener con el fin de hacer los resultados lo más intuitivos posible.

El funcionamiento de esta aplicación se recoge en la Figura 31.

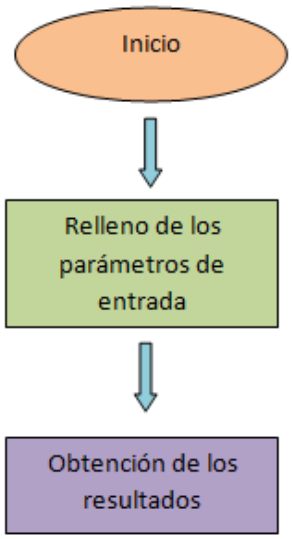


Figura 31: Diagrama de bloques del programa en Matlab.

5. EXPERIMENTOS REALIZADOS

5.1 Introducción

La esencia del proyecto es analizar como varía el rendimiento de un sistema de identificación biométrica cuando el reclutamiento y la identificación se realizan con sensores iguales y con sensores diferentes.

Para ello se realizarán dos tipos de pruebas de rendimiento, por un lado se procesará la BBDD para cada sensor, es decir, únicamente se compararán las imágenes de reclutamiento y de reconocimiento capturadas con el mismo sensor, a lo que denominaremos escenarios de igualdad. Por otro lado se procesará la BBDD cruzando las imágenes de dos sensores diferentes en cada prueba, es decir, el sensor utilizado para la captura de imágenes en el reclutamiento será diferente del sensor utilizado para la captura de las imágenes de reconocimiento, este escenario se denominará escenario de interoperabilidad.

Esto nos permitirá observar lo que ocurre con el rendimiento del sistema cuando se varía el sensor con el que se capturan las muestras de las visitas.

Por ello tendremos tres pruebas para cada uno de los tres sensores. Estas se organizaran en los dos escenarios mencionados en las secciones5.3.1 y 5.3.2.

En cada apartado de cada prueba se especifican los datos utilizados para la generación de los ficheros correspondientes a las nueve pruebas realizadas, 18 ficheros en total, 9 de genuinos y 9 de impostores. Además, se especifica cuáles son los ficheros incluidos para cada una de las pruebas realizadas en Matlab.

5.2 Experimentos realizados

Como se ha comentado anteriormente para analizar la interoperabilidad de los sensores de captura de huellas dactilares se han realizado diferentes pruebas, recogidas en dos escenarios, los escenarios de igualdad y los de interoperabilidad.

En los escenarios de igualdad todo el proceso de identificación biométrica de las personas mediante su huella dactilar se realiza con el mismo sensor. Sin embargo en los escenarios de interoperabilidad se utiliza un sensor para el reconocimiento diferente al que se utilizó para el reclutamiento.

A continuación se ofrece un resumen (Tabla 3) de las pruebas realizadas.

Tabla 3: Resumen de las pruebas realizadas.

Escenarios de igualdad		Escenarios de interoperabilidad	
Sensor utilizado en el reclutamiento	Sensor utilizado en el reconocimiento	**Sensor utilizado en el reclutamiento**	Sensor utilizado en el reconocimiento
NXT →	NXT	**NXT** →	FPC UPK
FPC →	FPC	**FPC** →	NXT UPK
UPK →	UPK	**UPK** →	NXT FPC

5.2.1 Escenarios de igualdad.

5.2.1.1 Prueba NXT-NXT

Para esta primera prueba en la ventana principal de la aplicación se activó tanto para el reclutamiento como para visitas el "checkbox" NXT. Por ello, la lista de imágenes de reclutamiento contenía todas las imágenes de reclutamiento capturadas con el sensor NXT de todos los usuarios, y la lista de imágenes de reconocimiento todas las imágenes de reconocimiento de todos los usuarios capturadas con NXT.

Dicho esto, en esta prueba se compararon todas las imágenes de reclutamiento del sensor NXT, con todas las imágenes de reconocimiento del sensor NXT.

Una vez la aplicación terminó de procesar todas las imágenes de todos los usuarios y guardar todos los resultados de comparación en los dos ficheros correspondientes generados en esta prueba (FicheroGenuinosNXT-NXT y FicheroImpostoresNXT-NXT), se rellenaron los vectores de clientes e impostores de la función EER_DET con los resultados de los ficheros creados. Específicamente el vector de "clients" se rellenó con los datos del FicheroGenuinosNXT-NXT y el vector de "impostors" se rellenó con los datos del FicheroImpostoresNXT-NXT.

5.2.1.2 Prueba FPC-FPC

Esta prueba sigue el mismo funcionamiento que la primera, cambiando el sensor NXT por el sensor FPC, por lo que en la ventana principal se eligió tanto para la muestra 1 como para la muestra 2 el sensor FPC, así, se compararon todas las imágenes de reclutamiento de FPC con todas las imágenes de reconocimiento de FPC.

5.2.1.3 Prueba UPK-UPK

Para el último escenario de igualdad se seleccionó en la ventana de inicio el sensor UPK para ambas muestras, del mismo modo que se realizó en las pruebas anteriores se compararon todas las muestras de reclutamiento del sensor UPK con todas las muestras de reconocimiento del mismo.

5.2.2 Escenarios de interoperabilidad.

Al igual que ocurría en las pruebas cuyo sensor de reclutamiento era el mismo que el de reconocimiento el proceso de generación de los ficheros y posteriormente el de las gráficas proporcionadas por Matlab es el mismo para cuando el sensor de reclutamiento no coincide con el sensor de reconocimiento. Por esta razón, el primer caso contendrá una explicación del proceso más detallada que en los casos siguientes, ya que lo único que varía de una prueba a otra son las imágenes que se incluyen en la lista de imágenes de reclutamiento y en la lista de reconocimiento y el nombre de los ficheros generados.

5.2.2.1 Sensor NXT

Este apartado recogen los resultados obtenidos cuando en la ventana principal se activó para la muestra 1 el "checkbox" cuya etiqueta contenía el nombre del sensor NXT y un sensor diferente del primero para la muestra 2, por lo que para este apartado las imágenes de la lista de reclutamiento únicamente serán las imágenes que estén recogidas con el sensor NXT y las imágenes de la lista de reconocimiento serán las capturadas con los dos sensores restantes.

5.2.2.1.1 Prueba NXT-FPC

Para esta prueba el "checkbox" activado en la ventana principal para las imágenes de reconocimiento fue el FPC, por lo que la lista de imágenes de reconocimiento se rellenó con todas las imágenes de reconocimiento capturadas con el sensor FPC. Se compararon las imágenes de reclutamiento de NXT con las imágenes de reconocimiento de FPC guardando los resultados de comparación de genuinos en FicheroGenuinosNXT-FPC y los resultados de comparación de impostores en FicheroImpostoresNXT-FPC. Una vez terminadas todas las comparaciones y rellenos los dos ficheros de esta prueba se adjudicaron los parámetros de entrada de la función EER_DET de la siguiente manera: el vector de "clients" se rellenó con el FicheroGenuinosNXT-FPC y el vector de "impostors" se llenó con los valores del FicheroImpostoresNXT-FPC.

5.2.2.1.2 Prueba NXT-UPK

La segunda prueba para el reclutamiento de NXT comparó las imágenes de reclutamiento de NXT con las imágenes de reconocimiento de UPK, por lo que al inicio del programa se activó el "checkbox" UPK para la muestra 2.

5.2.2.2 Sensor FPC

En este apartado el sensor utilizado para las imágenes de reclutamiento fue el sensor FPC. A continuación, se muestran las pruebas que se realizaron con un sensor diferente del FPC para la captura de las visitas.

5.2.2.2.1 Prueba FPC-NXT

Cuando se seleccionó para la muestra 2 el "checkbox" NXT, se compararon las imágenes de reclutamiento capturadas con FPC con las imágenes de reconocimiento capturadas con NXT.

5.2.2.2.2 Prueba FPC-UPK

Con la selección del "checkbox" UPK para la muestra 2 se compararon las imágenes de reclutamiento del sensor FPC con las imágenes de reconocimiento del sensor UPK

5.2.2.3 Sensor UPK

Por último, se utilizó como sensor para las imágenes de reclutamiento el sensor UPK, y al utilizar un sensor diferente para las imágenes de reconocimiento se obtuvieron las siguientes pruebas.

5.2.2.3.1 Prueba UPK-NXT

Para ésta primera prueba con el sensor de reclutamiento UPK se seleccionó en la ventana principal para la muestra 2 en sensor NXT, lo que hizo que se comparasen todas las imágenes de reclutamiento capturadas con el sensor UPK con todas las imágenes de reconocimiento capturadas con el sensor NXT.

5.2.2.3.2 Prueba UPK- FPC

En esta última prueba se seleccionó el sensor FPC como sensor de la muestra 2, por lo que en esta última prueba se compararon las imágenes de reclutamiento recogidas con el sensor UPK con las imágenes de reconocimiento recogidas con el sensor FPC.

5.3 Análisis de los resultados

Como se ha comentado en el apartado de rendimiento de una evaluación biométrica, 2.1.3.5, existen diferentes tasas de error. Para analizar el rendimiento de los sistemas objeto de este TFG se han estudiado algunos de los porcentajes de error de los diferentes sistemas.

Estos porcentajes pueden ser mostrados de varias maneras:

FRR = FTA + FNMR
FAR = FTA+ FMR

- El porcentaje FRR, "False Reject Rate", mide la proporción de identificaciones genuinas para las cuales el sujeto es rechazado. Este porcentaje está formado por la suma de:

  - El porcentaje de intentos de reconocimiento para los cuales el sistema falla al intentar adquirir muestras con suficiente calidad, FTA. En este proyecto se supondrá que los errores, FTA son aquellos comentados en el apartado 3.4.1.1.3, es decir aquellos que presentan un cero en el resultado de comparación.

  - El porcentaje de intentos de reconocimiento de genuinos para los cuales el sujeto es rechazado, es decir, la tasa FNMR

- De la misma manera el porcentaje FAR, "False Accept Rate", porcentaje de identificaciones de impostor para las cuales el sujeto es aceptado, está formado por la suma del porcentaje FTA, explicado para el caso anterior y del porcentaje FMR, "False Match Rate", mide la proporción de intentos de reconocimiento de impostor para los cuales el sujeto es aceptado.

Existen análisis biométricos en los que las muestras cuyo número de minucias es cero, porcentaje FTA, se tratan como un error y no participan en dicho análisis, entonces, los errores FRR y FAR son iguales a los errores FNMR y FMR, respectivamente.

En este proyecto se proporcionan para cada prueba primero los resultados de las pruebas cuando se tienen en cuenta los errores de FTA , porcentajes FRR y FAR, y posteriormente se eliminarán dichos errores y se ofrecerán las gráficas sin los FTA, por lo que se obtienen los valores de FMNR y FMR.

Con el fin de valorar qué sistema obtiene más errores FTA se proporcionarán para cada prueba su porcentaje.

Como se ha comentado en el apartado 3.4.2.2, mediante la función EER_DET se obtienen dos curvas y dos valores, todos ellos se representan mediante tres graficas: en la primera se muestra el valor EER, en la segunda la curva DET y la tercera está destinada a mostrar la curva ROC.

Con el fin de poder analizar los resultados con mayor facilidad estos se han dispuesto de la siguiente manera:

- Primero se ofrecen dos gráficas, para cada uno de los tres escenarios de igualdad, donde se muestra el punto EER de la tasas FRR vs FAR y FMR vs FNMR.

  En este apartado también se ofrece una gráfica donde se incluyen tres curvas DET y tres curvas ROC cada una corresponde a uno de los tres escenarios de igualdad con el fin de observar cuál de los tres sensores tiene menor porcentaje de error y en consecuencia mayor rendimiento. El rendimiento de un sensor se determina comparando sus muestras de reclutamiento con sus muestras de las visitas

El incluir primero las gráficas de los escenarios de igualdad es debido a que cuando se utiliza un sensor para el reconocimiento diferente al que se utilizó para el reclutamiento pueden darse dos casos:

El primero supone que el sensor utilizado para la captura de las imágenes de reconocimiento tenga un rendimiento superior al que se utilizó para la captura de las imágenes de reclutamiento. Esto provoca que al mezclar información obtenida por estos dos sensores el rendimiento del conjunto aumente con respecto al rendimiento del sensor de reclutamiento.

Sin embargo, si el sensor utilizado para la captura durante el reconocimiento posee un rendimiento peor con respecto al de las imágenes de reclutamiento el rendimiento del conjunto disminuye con respecto al del primero.

Por ello, si se sabe el rendimiento de cada sensor será más fácil analizar como varía el rendimiento según los cruces de los sensores.

- Segundo se ofrecen dos gráficas para cada una de los seis escenarios de interoperabilidad, donde se muestra el valor EER de la tasas FRR vs FAR y FMR vs FNMR.

  Estas seis pruebas restantes están separadas en tres bloques, cada uno correspondiente al sensor de reclutamiento utilizado en la comparación.

  Al final de cada bloque se ofrecen dos gráficas más donde se incluyen tres curvas DET y ROC correspondientes al escenario de igualdad del sensor de reclutamiento y las otras dos a los escenarios de interoperabilidad para ese mismo sensor.

  Esta última gráfica de cada bloque se genera con el fin de observar de manera más sencilla como aumenta o disminuye el rendimiento de un sensor cuando se cruzan sus imágenes con las de los otros dos sensores.

En los escenarios de igualdad como en los de interoperabilidad, las gráficas destinadas a mostrar los resultados tanto de las tasas FRR y FAR como de las FNMR y FMR, y en consecuencia el punto EER de cada prueba, representarán en el eje de ordenadas, eje Y, el error y en el eje de abscisas, eje X, el umbral, como se muestra en la Figura 32.

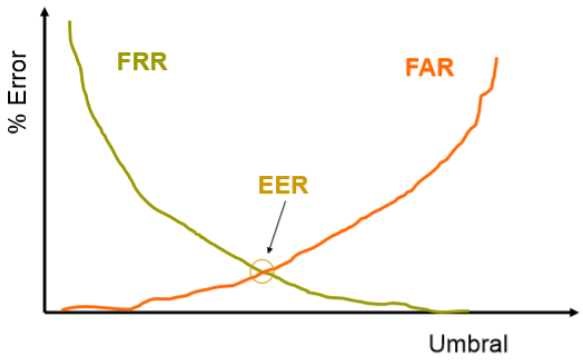


Figura 32: Ejes de las gráficas destinadas a representar el punto EER [37]

5.3.1 Rendimiento de los escenarios de igualdad

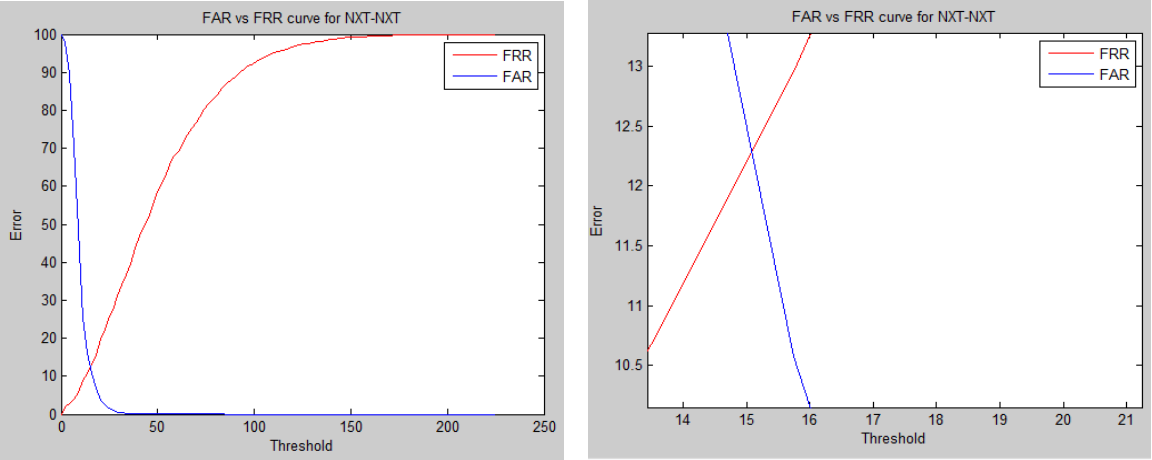
En este apartado se busca obtener el EER de cada uno de los tres sensores, para ello se han realizado tres pruebas, donde las imágenes de reclutamiento y las imágenes de reconocimiento están capturadas con el mismo sensor.

Dado que los resultados de rendimiento biométrico están basados en probabilidades, antes de mostrar los mismos se ofrece la Tabla 4 donde se muestra el número de comparaciones realizadas para los escenarios de igualdad.

Tabla 4: Número de comparaciones de los escenarios de igualdad.

	NXT	FPC	UPK
Genuinos	3.908	4.053	3.879
Impostores	1.222.401	1.279.039	1.184.909

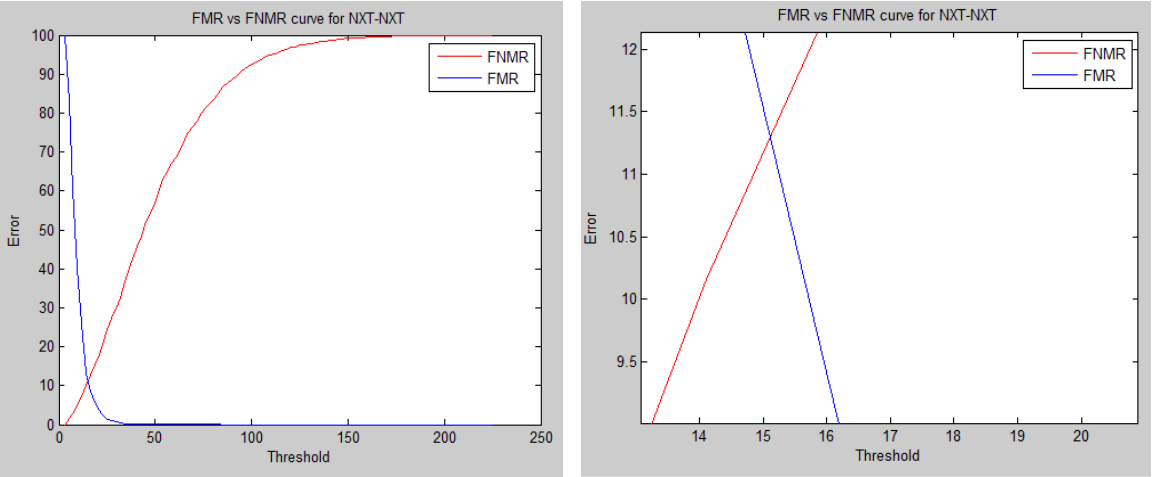
Resultados del punto EER para la prueba NXT-NXT



(a) (b)

Figura 33: Curva FRR vs FAR para el sensor NXT.

(a) Gráfica completa.
(b) Zoom del punto EER.



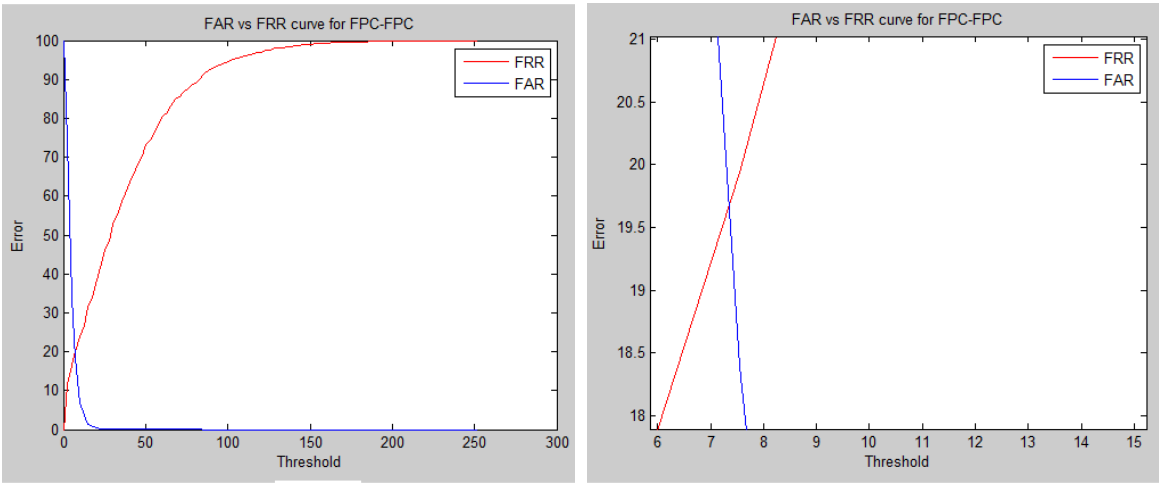
(a) (b)

Figura 34: Curva FMR vs FNMR para el sensor NXT.

(a) Gráfica completa.
(b) Zoom del punto EER.

Como se observa en las dos imágenes anteriores al eliminar la tasa de errores FTA el error disminuye, al no incluir el error FTA, con lo que el rendimiento y seguridad del sistema aumentan.

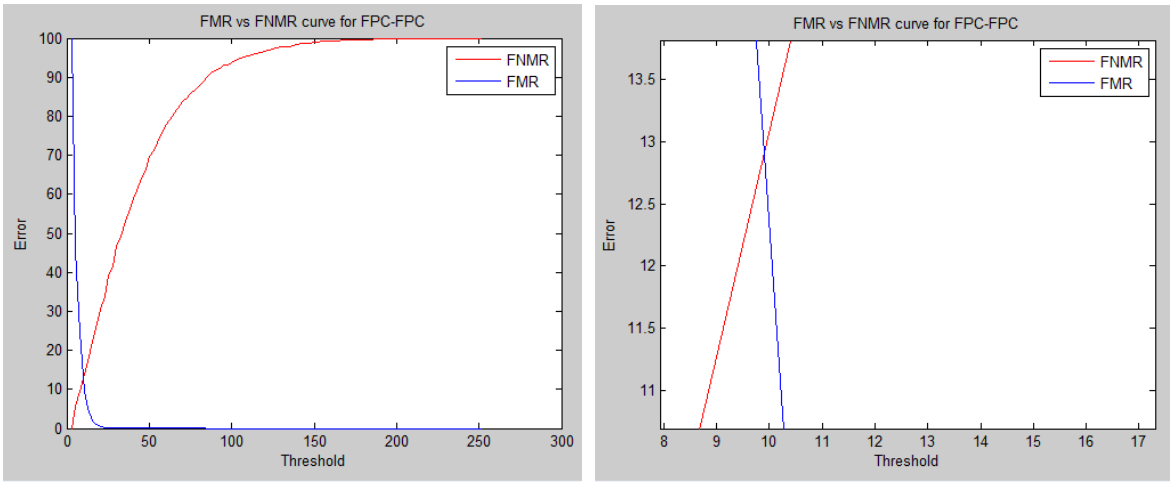
Resultados del punto EER para la prueba FPC-FPC



(a) (b)

Figura 35: Curva FAR vs FRR para el sensor FPC.

(a) Gráfica completa.
(b) Zoom del punto EER.



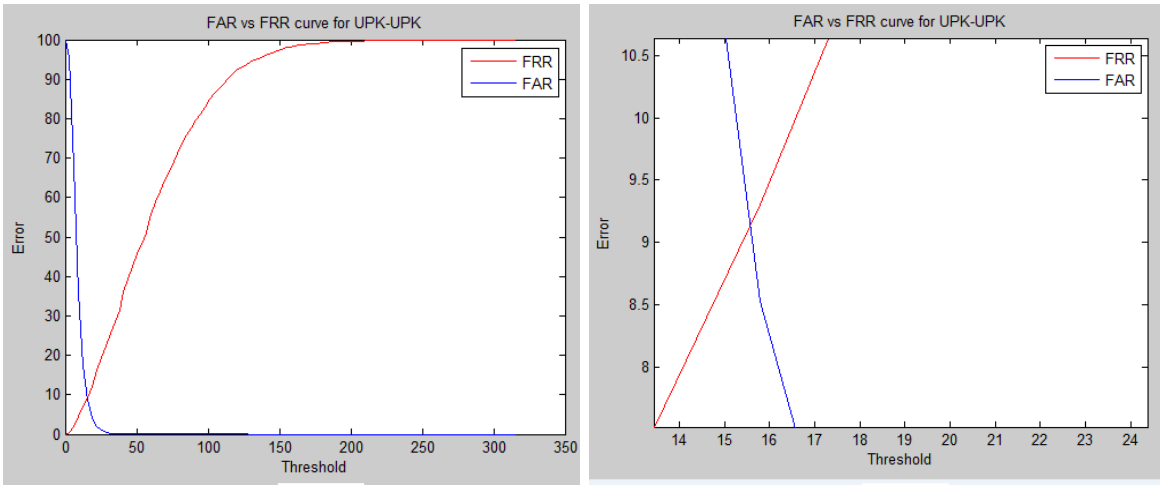
(a) (b)

Figura 36: Curva FMR vs FNMR para el sensor FPC.

(a) Gráfica completa.
(b) Zoom del punto EER.

De la misma manera que ocurre en el caso anterior, al eliminar los errores FTA disminuye el error del sistema, lo que hace aumente la seguridad y rendimiento del mismo.

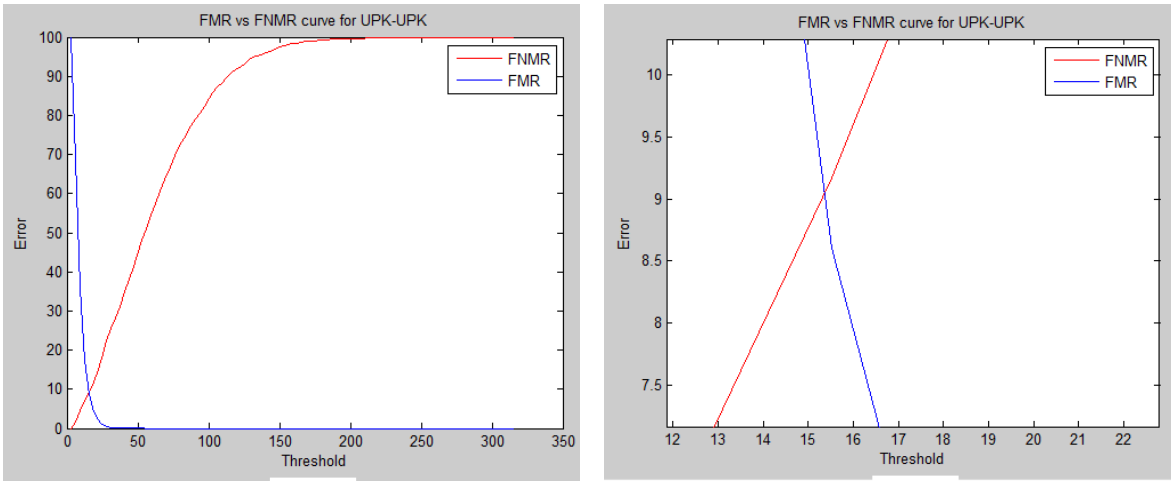
Resultados del punto EER para la prueba UPK-UPK



(a) (b)

Figura 37: Curva FAR vs FRR para el sensor UPK.

(a) Gráfica completa.
(b) Zoom del punto EER.



(a) (b)

Figura 38: Curva FMR vs FNMR para el sensor UPK.

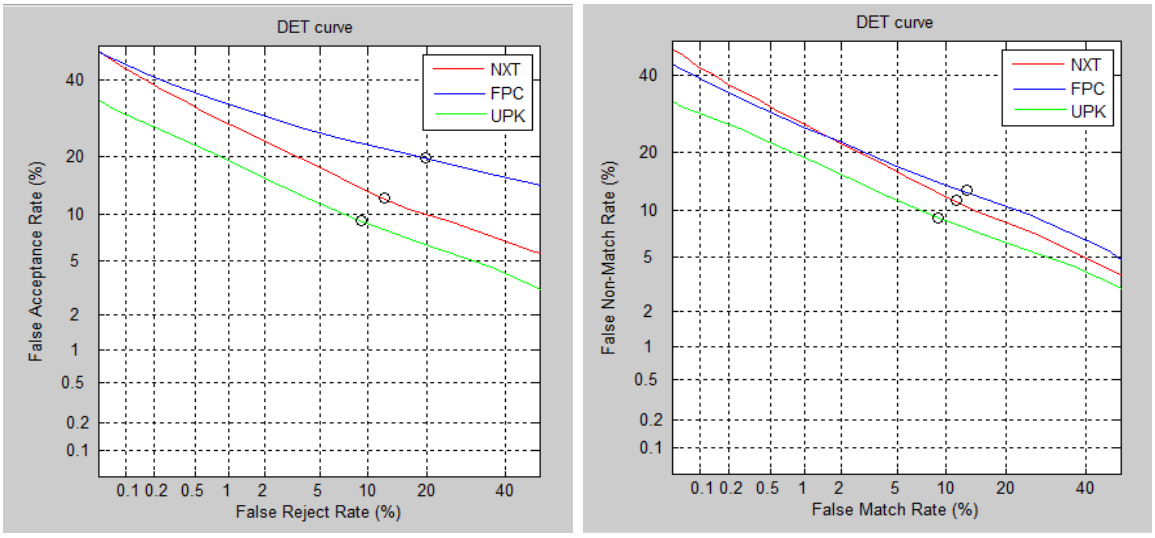
(a) Gráfica completa.
(b) Zoom del punto EER.

Para este caso, el porcentaje de error adquiere un valor muy similar en ambos casos, por lo que este sensor posee errores de FTA muy bajos.

Se ha modificado la función EER_DET con el fin de conseguir cuatro gráficas más, dos para las curvas DET y las otras dos para las curvas ROC, todas ellas de los tres escenarios de igualdad, para ofrecer una visión grafica conjunta de los errores de los sistemas.

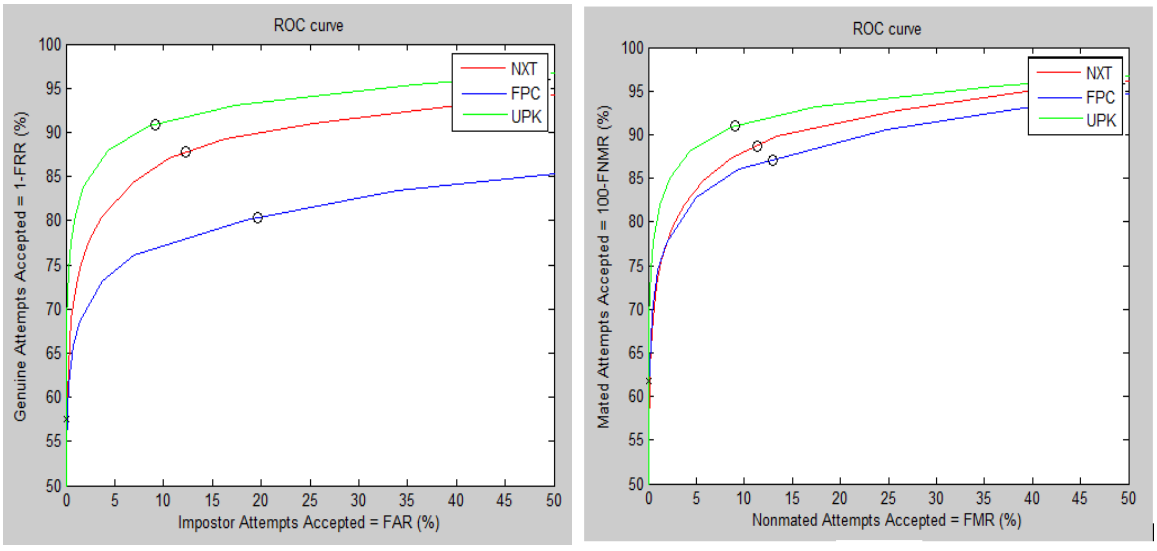
Para estas últimas gráficas se han incluido simultáneamente en la función EER_DET los ficheros de genuinos e impostores de las combinaciones NXT- NXT, FPC-FPC y UPK- UPK.

Resultados de las curvas DET para los escenarios de igualdad.



(a) (b)

Figura 39: Curvas DET para escenarios de igualdad.
(a) FRR-FAR
(b) FNMR-FMR.



(a) (b)

Figura 40: Curvas ROC para escenarios de igualdad.
(a) FRR-FAR
(b) FNMR-FMR.

Como se aprecia en los apartados (a) de las Figuras 39 y 40 el sensor FPC posee, con diferencia, el mayor porcentaje de errores de FAR y FRR, lo que hace que su comportamiento se aleje del de los otros dos sensores, quienes poseen estos porcentajes en menor medida y con mayor semejanza entre ellos.

FPC también posee el porcentaje FTA más alto, lo que hace que tras la eliminación de este el comportamiento de FPC se asemeje al de los otros dos sensores, como se aprecia en los apartados (b) de las Figuras 39 y 40.

Por último se ofrece la Tabla 5 donde se resumen los porcentajes de error de los tres sensores utilizados, primero teniendo en cuenta el porcentaje de FTA y, a continuación, haciendo este porcentaje nulo, con el fin de obtener los porcentajes de FTA para cada uno de los sensores. Este porcentaje se calcula según las siguientes expresiones:

FAR = FTA+ FMR
FRR = FTA + FNMR

Tabla 5: Comparativa de los resultados para los escenarios de igualdad.

	EER(FAR vs FRR)	EER(FMR vs FNMR)	FTA
NXT	12.2%	11.5%	0.7%
FPC	19.75%	12.8%	8.05%
UPK	9.2%	9.1%	0.1%

Como se observa en la Tabla 5 el sensor con mayor porcentaje de error FTA es el FPC, seguido del NXT y este del UPK, quien ofrece un porcentaje FTA muy reducido.

De aquí se puede deducir que el sensor FPC comete un gran número de errores al intentar adquirir muestras con suficiente calidad, a diferencia del sensor UPK quien comete un número de errores muy reducido.

5.3.2 Rendimiento de los escenarios de interoperabilidad

Una vez evaluado el rendimiento de cada uno de los sensores utilizados se procedió a crear seis nuevos sistemas, en los que los sensores utilizados para capturar las imágenes de reclutamiento son diferentes de los utilizados para la captura de las imágenes de reconocimiento.

En este aparatado se va a valorar que le ocurre al rendimiento del sensor de reclutamiento cuando se utiliza un sensor diferente de este para la captura de las imágenes de reconocimiento.

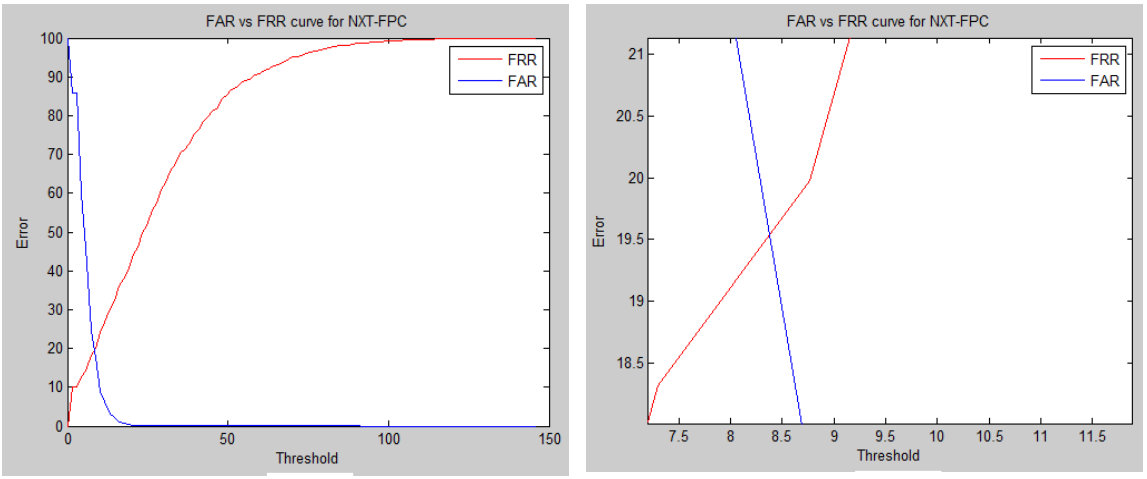
En las seis pruebas siguientes se dará, al igual que en las tres anteriores, el punto EER en dos situaciones diferentes, primero teniendo en cuenta la tasa de error FTA y posteriormente eliminando los datos que forman esta tasa.

También se ofrece la Tabla 6 donde se recoge el número de comparaciones realizadas para cada prueba.

Tabla 6: Número de comparaciones de escenarios de interoperabilidad

	NXT-FPC	NXT-UPK	FPC-NXT	FPC-UPK	UPK-NXT	UPK-FPC
Genuinos	4.400	3.982	3.690	3.764	3.802	4.147
Impostores	1.390.540	1.218.531	1.159.236	1.155.577	1.188.682	1.311.584

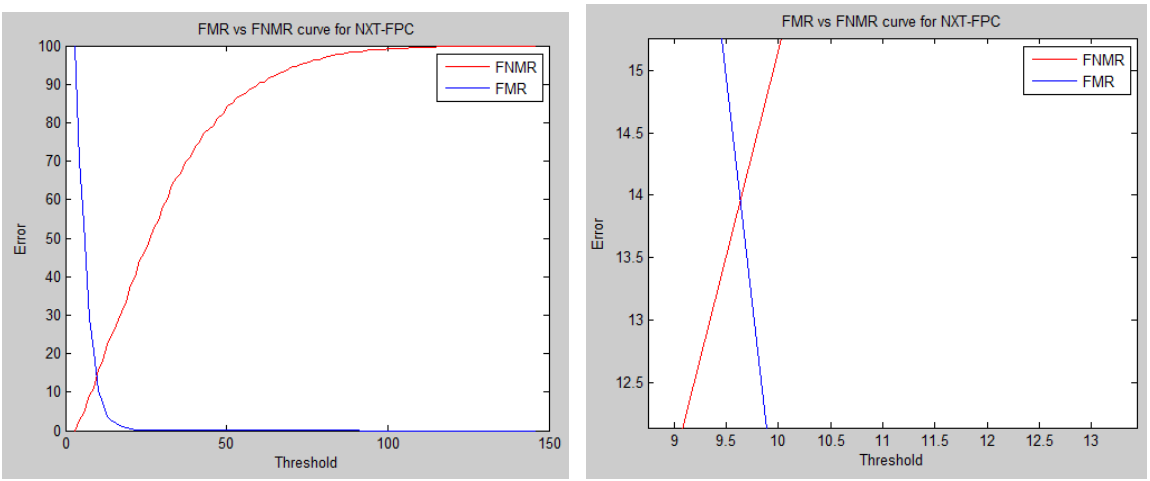
Resultados del punto EER para la prueba NXT-FPC



(a) (b)

Figura 41: Curva FRR vs FAR para el sistema NXT-FPC.

(a) Gráfica completa.
(b) Zoom del punto EER.



(a) (b)

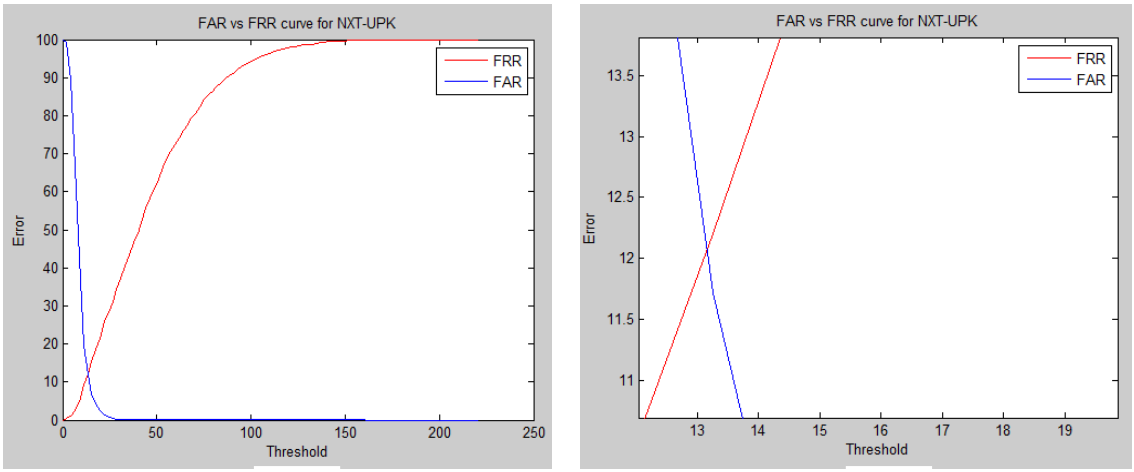
Figura 42: Curva FMR vs FNMR para el sistema NXT-FPC.

(a) Gráfica completa.
(b) Zoom del punto EER.

En estas imágenes se muestran los puntos EER del sistema NXT-FPC para las dos situaciones comentadas (con error FTA y sin error FTA).

Para ambos casos el porcentaje de error del sistema aumenta con respecto al porcentaje del sistema NXT-NXT. Esto se debe a que el sensor de reconocimiento es el FPC, quien posee un porcentaje de error superior en ambos casos al del NXT, por lo que al utilizar este sensor en las imágenes de visitas hace que el sistema aumente sus tasas de error con respeto a las de NXT.

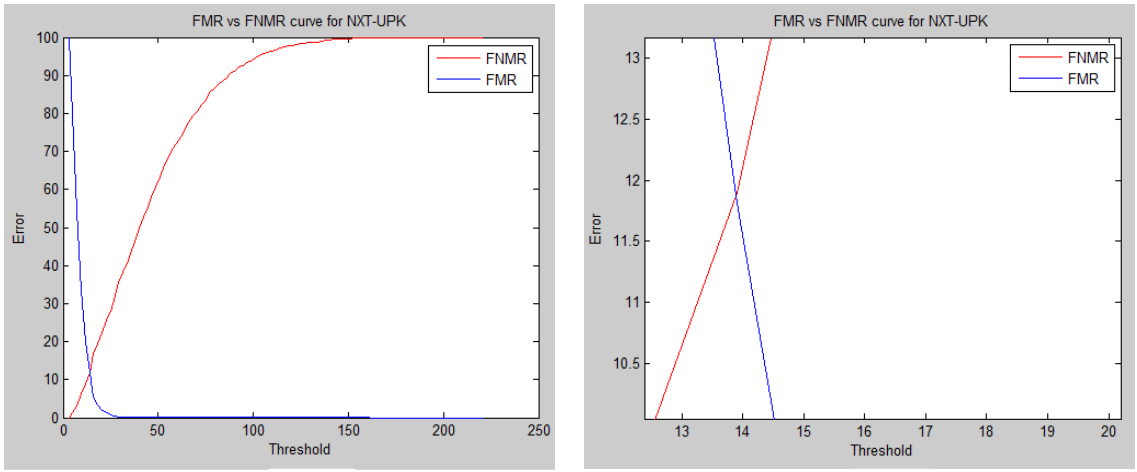
Resultados del punto EER para la prueba NXT-UPK



(a) (b)

Figura 43: Curva FRR vs FAR para el sistema NXT-UPK.

(a) Gráfica completa.
(b) Zoom del punto EER.



(a) (b)

Figura 44: Curva FMR vs FNMR para el sistema NXT-UPK.

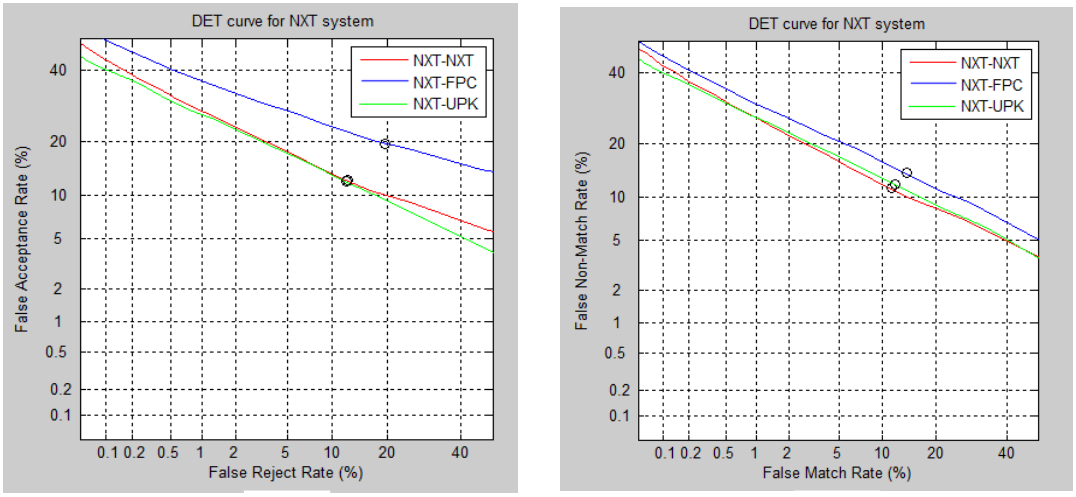
(a) Gráfica completa.
(b) Zoom del punto EER.

En la primera situación, la tasa de errores disminuye con respecto al sistema NXT-NXT. Esto es debido a que el segundo sensor, UPK, proporciona imágenes de mejor calidad que el NXT, por lo que al utilizarlo en el reconocimiento hace que las tasas de error del sistema disminuyan con respecto a las del primero.

En la segunda situación, una vez eliminados los errores FTA, que tienen que ver con la calidad de la muestra se da el caso contrario respecto a la prueba NXT-NXT, el porcentaje de errores aumenta levemente a pesar de que el sensor UPK proporciona imágenes de mejor calidad.

A continuación se muestran las graficas DET y ROC, de las dos situaciones, para los tres casos en los que el sensor de reclutamiento es el NXT.

Resultados de las curvas DET para el sistema NXT.

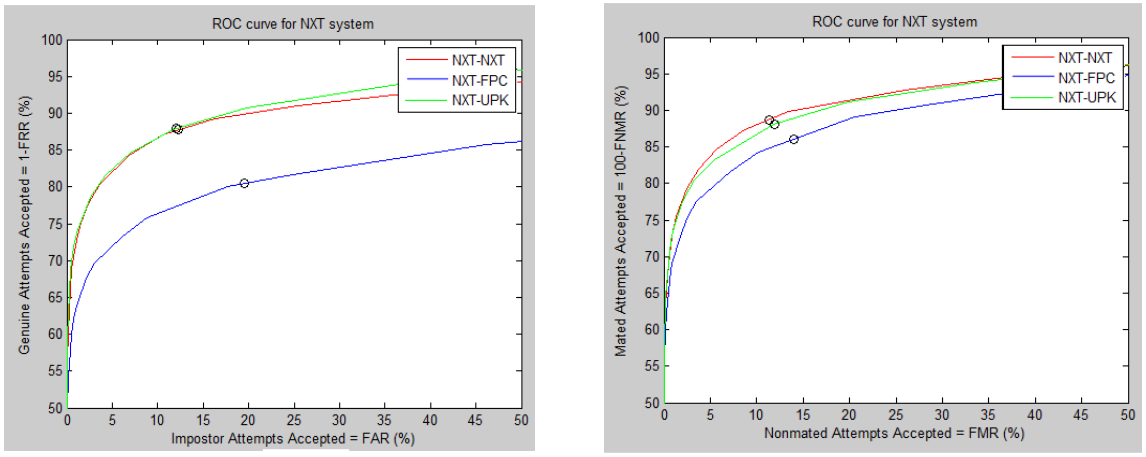


(a) (b)

Figura 45: Curvas DET para el sistema NXT.

(a) FRR-FAR
(b) FNMR-FMR.

Resultados de las curvas ROC para el sistema NXT.



(a) (b)

Figura 46: Curvas ROC para el sistema NXT.

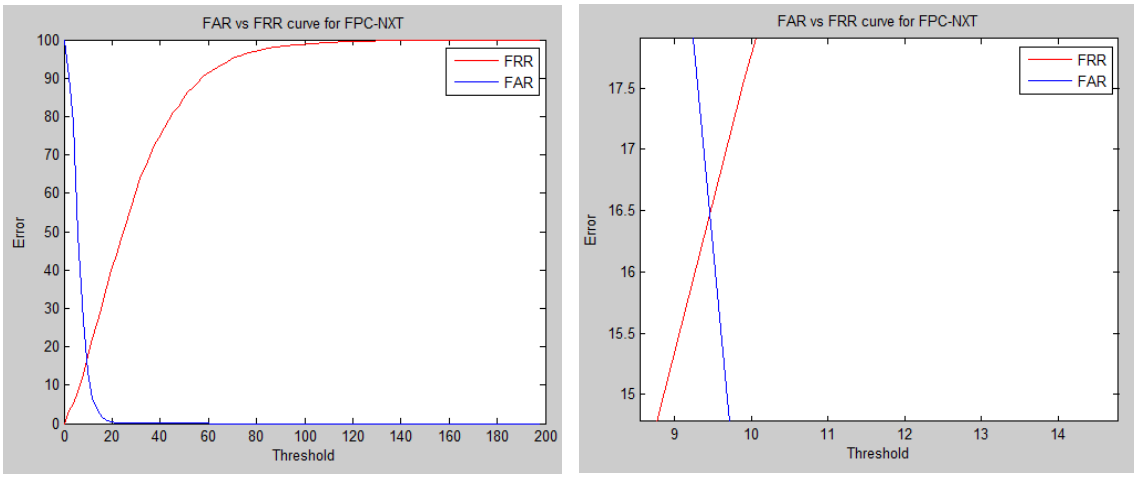
(a) FRR-FAR
(b) FNMR-FMR.

Se puede apreciar de una manera más intuitiva tras las uniones de las gráficas, que, teniendo en cuenta los errores FTA, el utilizar un sensor de captura que proporciona imágenes con peor calidad para la comparación que el utilizado en el reclutamiento, implica que los errores del nuevo sistema aumenten.

Si por el contrario se utiliza un sensor que proporciona imágenes con mejor calidad el rendimiento del sistema aumenta.

Si se observan las gráficas en las que los errores FTA no han participado en el análisis se aprecia que tanto para la unión del sensor NXT con FPC como para la unión de este primero con el sensor UPK las tasas de errores aumentan, lo que provoca que ambos sistemas posean un rendimiento inferior al que posee el sistema NXT-NXT.

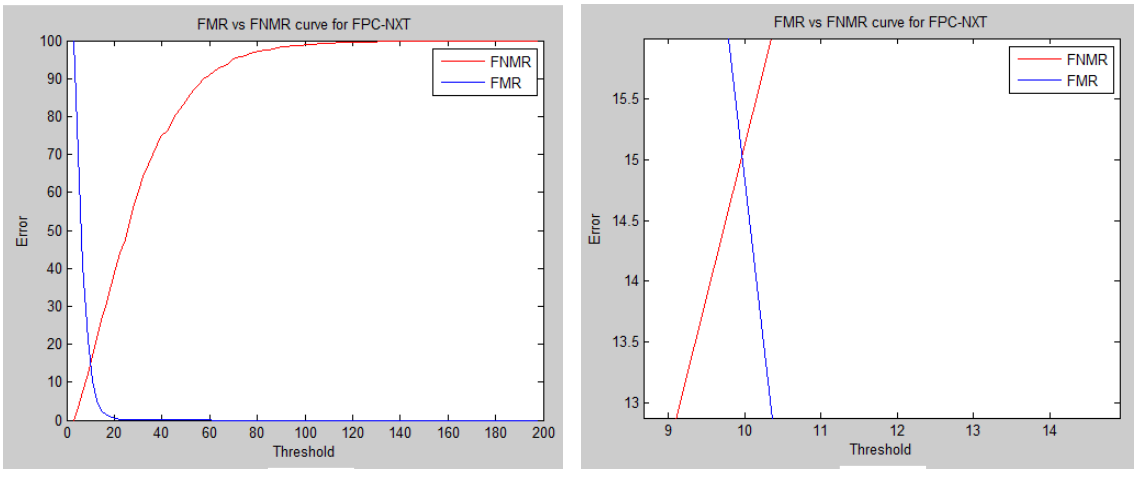
Resultados del punto EER para la prueba FPC-NXT



(a) (b)

Figura 47: Curva FRR vs FAR para el sistema FPC-NXT.

(a) Gráfica completa.
(b) Zoom del punto EER.



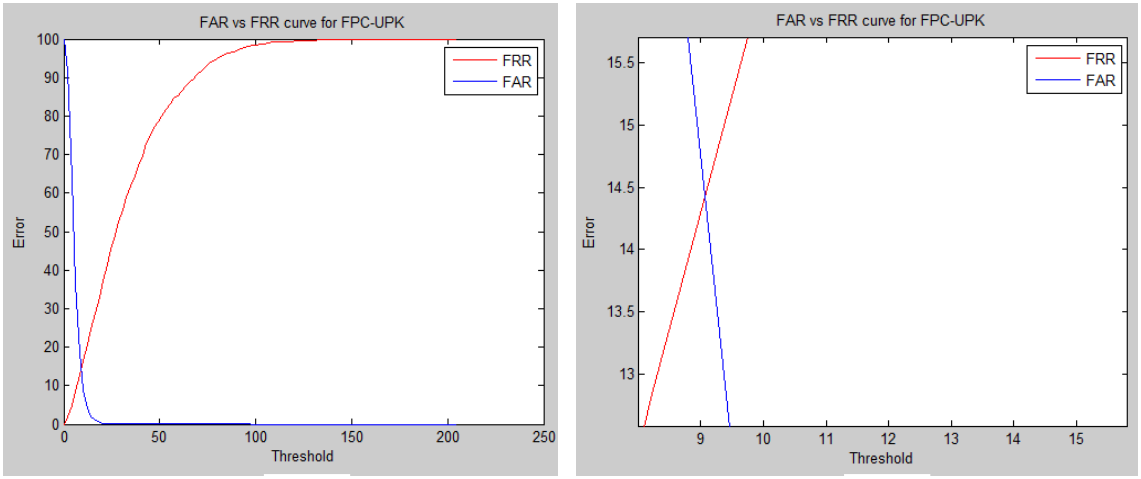
(a) (b)

Figura 48: Curva FMR vs FNMR para el sistema FPC-NXT.

(a) Gráfica completa.
(b) Zoom del punto EER.

Se observa que en la primera situación el sistema disminuye las tasas de error con respecto al sistema de comparación en igualdad FPC-FPC, sin embargo, cuando se elimina la tasa FTA, las tasas de error del conjunto aumentan con respecto a las tasas de error del sistema FPC-FPC, a pesar de utilizar en el reconocimiento un sensor que proporciona imágenes de mejor calidad que el sensor FPC, sensor utilizado en el reclutamiento.

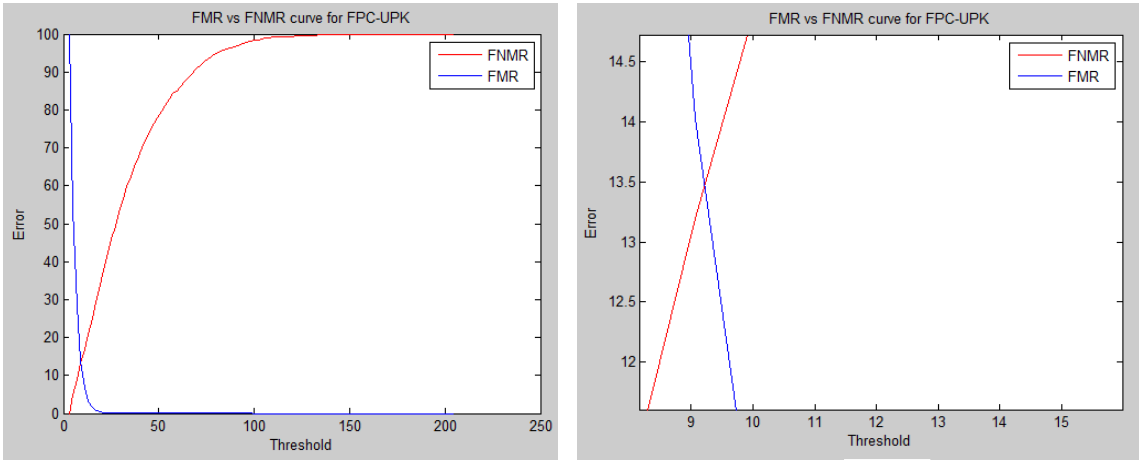
Resultados del punto EER para la prueba FPC-UPK



(a) (b)

Figura 49: Curva FRR vs FAR para el sistema FPC-UPK.

(a) Gráfica completa.
(b) Zoom del punto EER.



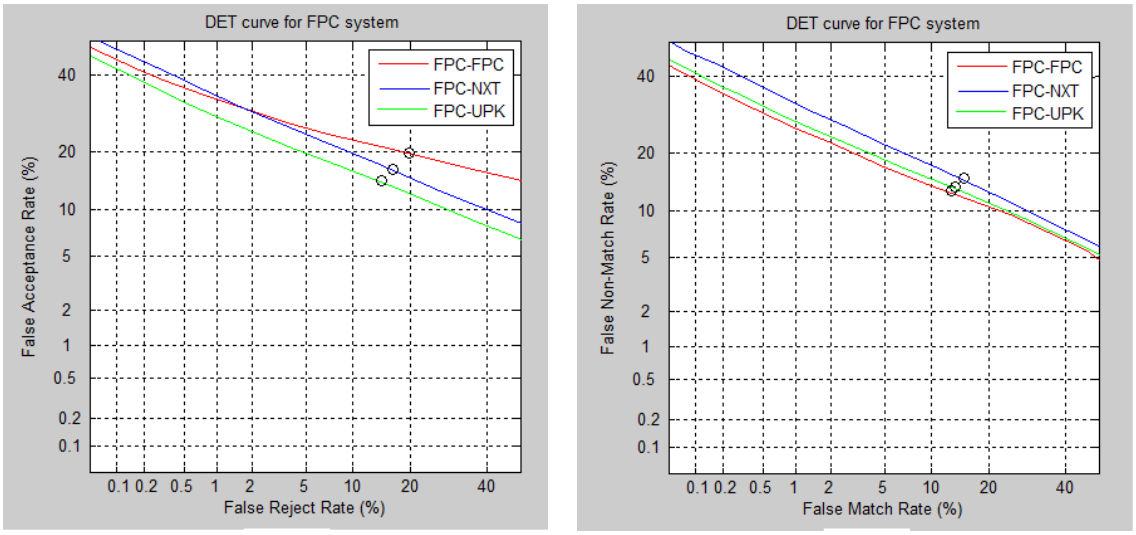
(a) (b)

Figura 50: Curva FMR vs FNMR para el sistema FPC-UPK.

(a) Gráfica completa.
(b) Zoom del punto EER.

Estas imágenes reflejan los puntos EER del sistema FPC-UPK. En esta prueba se da el mismo caso que en la prueba anterior, prueba FPC-NXT, en la primera situación el error del conjunto disminuye excesivamente con respecto sistema FPC-FPC. Sin embargo en la segunda situación, el rendimiento del sistema disminuye con respecto al sistema FPC-FPC.

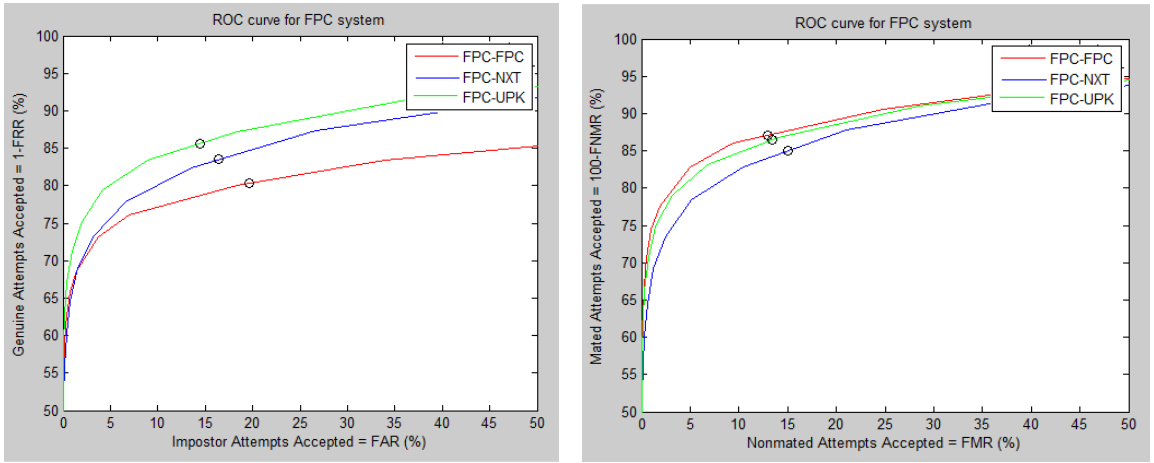
Como para el caso del sistema NXT, se ofrecen, de la misma manera, cuatro gráficas, dos DET y las otras dos ROC, cada una muestra una de las dos situaciones.



(a) (b)

Figura 51: Curvas DET para el sistema FPC.

(a) FRR-FAR
(b) FNMR-FMR.



(a) (b)

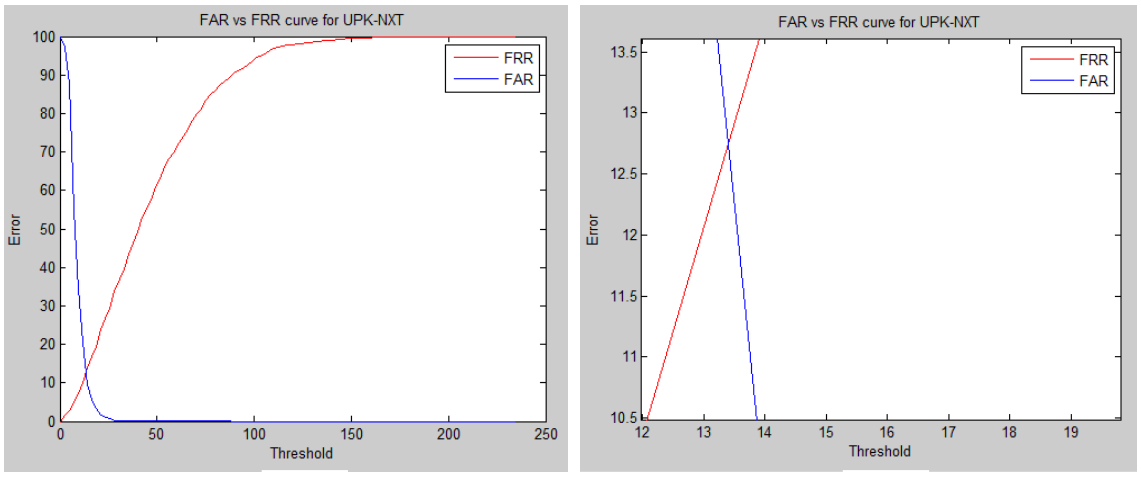
Figura 52: Curvas ROC para el sistema NXT.

(a) FRR-FAR
(b) FNMR-FMR.

En estas dos pruebas se da la misma situación que en la prueba NXT-UPK, cuando se incluyen los valores FTA en el análisis el rendimiento de los sistemas disminuye, ya que los sensores utilizados en el reconocimiento proporcionan imágenes de mejor calidad que el sensor FPC, sensor de reclutamiento.

Sin embargo, cuando los errores FTA son eliminados los resultados son los contrarios, es decir, las tasas de error aumentan con respecto a las tasas de error del sistema FPC-FPC a pesar de ser los sensores de reconocimiento sensores que obtienen imágenes de mejor calidad que el FPC:

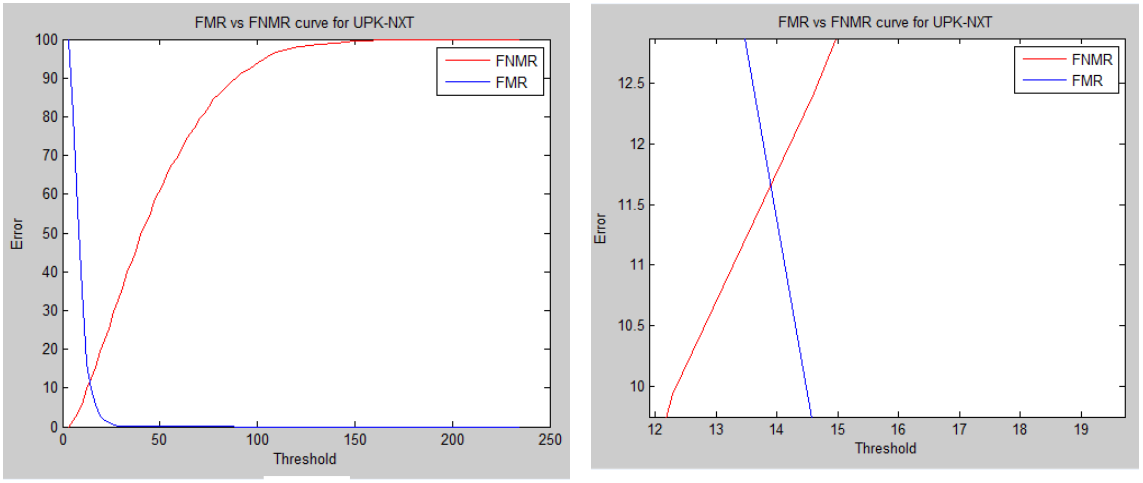
Resultados del punto EER para la prueba UPK-NXT



(a) (b)

Figura 53: Curva FRR vs FAR para el sistema UPK-NXT.

(a) Gráfica completa.
(b) Zoom del punto EER.



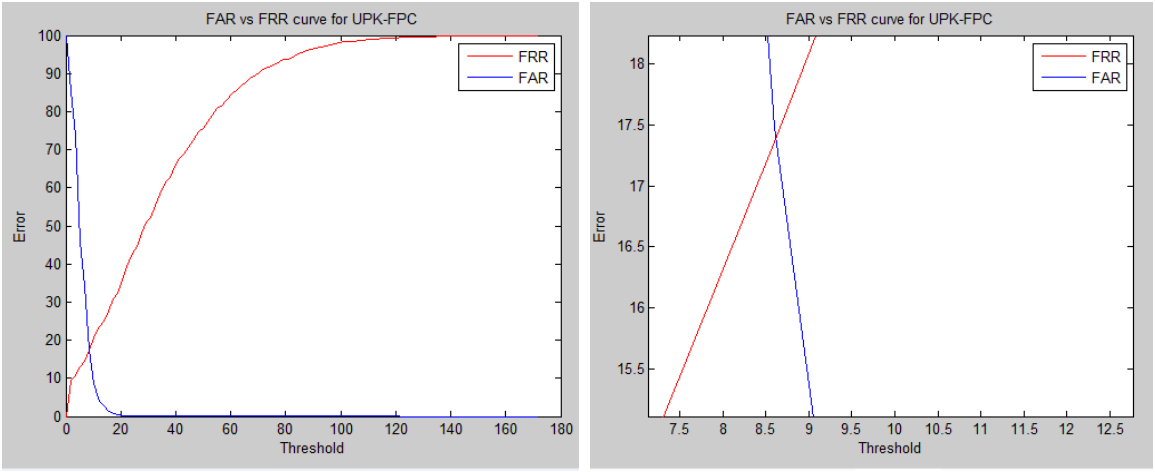
(a) (b)

Figura 54: Curva FMR vs FNMR para el sistema UPK-NXT.

(a) Gráfica completa.
(b) Zoom del punto EER.

En estas gráficas se ofrecen los puntos EER para el sistema UPK-NXT.
En este sistema se observa como el error del conjunto aumenta con respecto al sistema UPK-UPK, ya que el sensor NXT tiene un porcentaje de error mayor que el UPK.

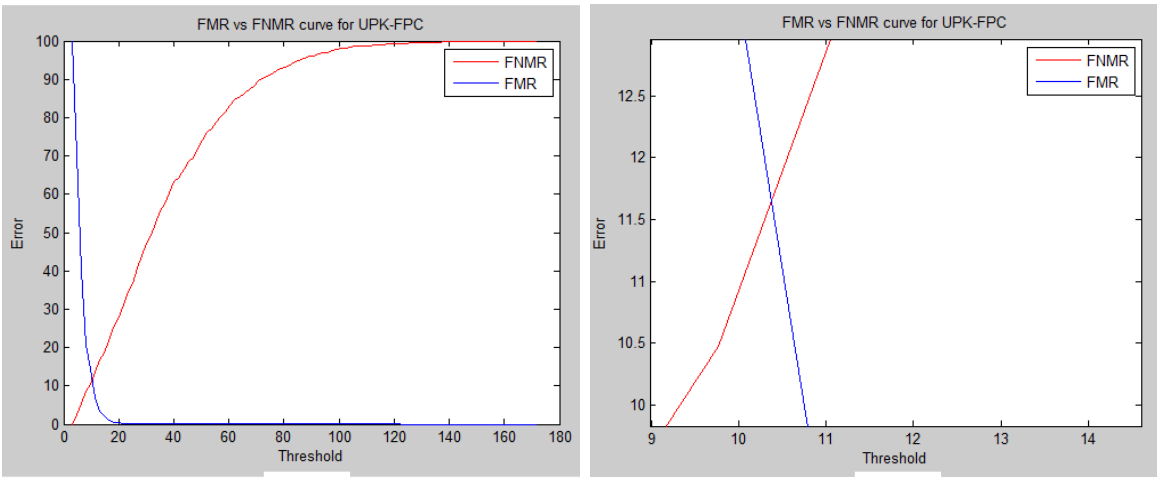
Resultados del punto EER para la prueba UPK-FPC



(a) (b)

Figura 55: Curva FRR vs FAR para el sistema UPK-FPC.

(a) Gráfica completa.
(b) Zoom del punto EER.



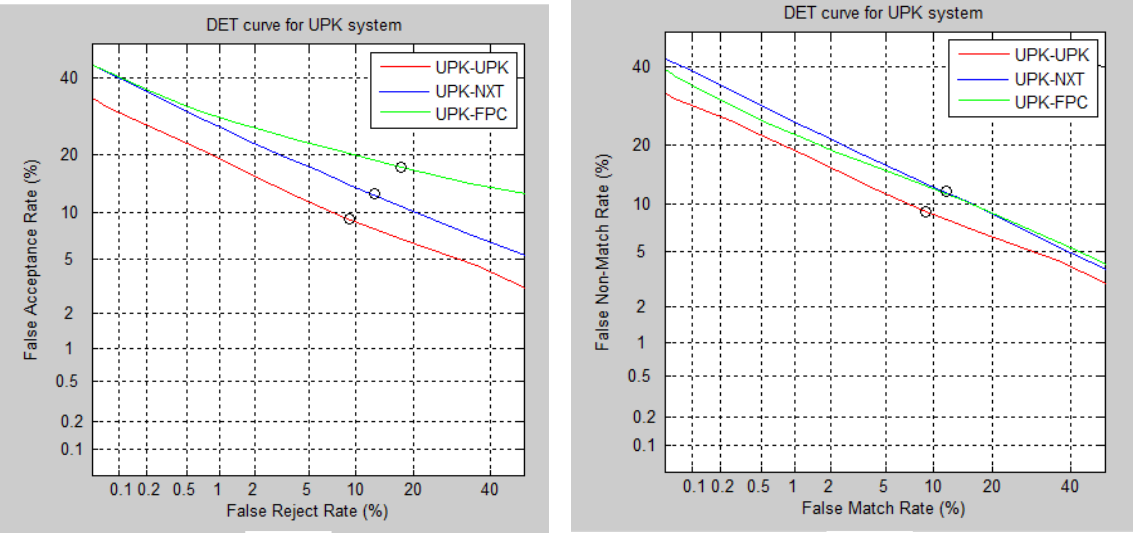
(a) (b)

Figura 56: Curva FMR vs FNMR para el sistema UPK-FPC.

(a) Gráfica completa.
(b) Zoom del punto EER.

Para este sistema el porcentaje de error aumenta con respecto al porcentaje de error en las comparaciones UPK-UPK, ya que el sensor de visitas es el FPC, el cual proporciona imágenes de peor calidad que el sensor UPK.

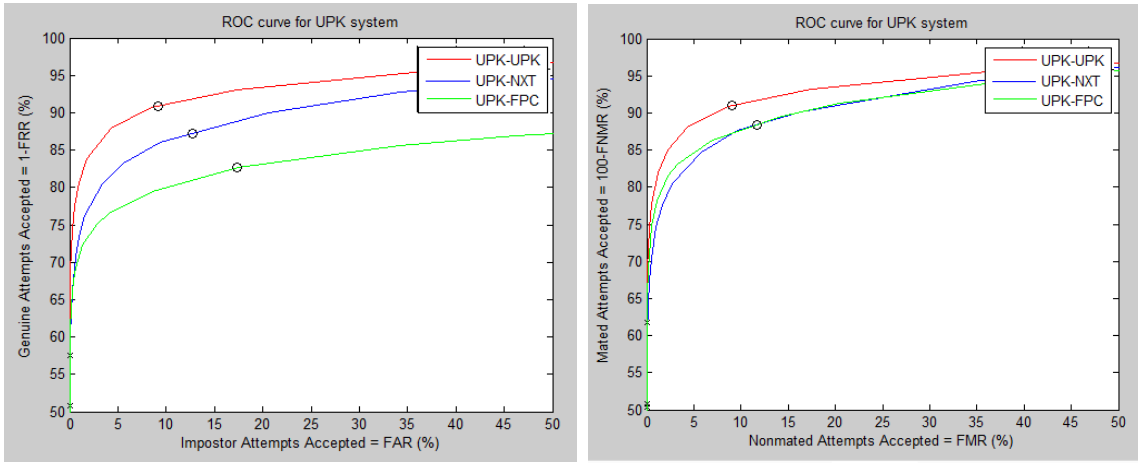
Al igual que en las pruebas anteriores se ofrecen las graficas DET y ROC del sistema UPK, con el fin de evaluarlo de forma conjunta.



(a) (b)

Figura 57: Curvas DET para el sistema UPK.

(a) FRR-FAR
(b) FNMR-FMR.



(a) (b)

Figura 58: Curvas ROC para el sistema UPK.

(a) FRR-FAR
(b) FNMR-FMR.

En estas dos últimas pruebas el porcentaje de errores ha aumentado con respecto al porcentaje que posee el sistema UPK-UPK, ya que el sensor UPK proporciona imágenes mejores respecto a los otros dos sensores. De tal forma que al juntarlo con cualquiera de los otros dos el rendimiento del conjunto disminuye debido al aumento de los errores.

5.3.3 Conclusiones de ambos escenarios

Tras conocer el rendimiento de los nueve sistemas analizados, primero los tres pertenecientes a los escenarios de igualdad y posteriormente los seis restantes, pertenecientes a los escenarios de interoperabilidad, se puede observar que, teniendo en cuenta los errores FTA, el rendimiento de un sistema formado por dos sensores diferentes varía con respecto al rendimiento del sensor de reclutamiento del sistema de la siguiente manera:

- Si el sensor de reconocimiento proporciona imágenes de peor calidad que el del reclutamiento, el rendimiento del conjunto disminuye, como se da en el caso de las pruebas con UPK. UPK es el sensor que mejor calidad de imágenes obtiene, sin embargo, cuando se forma un sistema donde el sensor de reclutamiento es el UPK, pero el de reconocimiento es NXT o FPC, los errores del conjunto aumentan como se aprecia en las Figuras 57 y 58, por lo que el rendimiento del conjunto disminuye.

- Si el sensor de reconocimiento presenta imágenes de mejor calidad el rendimiento del conjunto aumenta. Esto se aprecia en el caso del sensor FPC, dado que este sensor presenta las tasas de error más elevadas de los tres. Como se observa en las Figuras 51 y 52 al formar un sistema cuyo sensor de reclutamiento es el FPC, pero el sensor de reconocimiento es el NXT o el UPK el rendimiento de dicho sistema aumenta con respecto al que tenia FPC.

Pero los resultados no son los mismos cuando se eliminan los errores FTA, dado que sin tener en cuenta estos datos el rendimiento de cualquiera de los sistemas formados por dos sensores diferentes posee un rendimiento inferior que aquellos sistemas en los que el sensor de reclutamiento es el mismo que el de reconocimiento. Esto se puede apreciar en los sistemas NXT-UPK, FPC-NXT y FPC-UPK, dado que al incluir los errores FTA el rendimiento del sistema aumenta con respecto al rendimiento en igualdad NXT-NXT o FPC-FPC, ya que el sensor de reconocimiento obtiene imágenes de mejor calidad, sin embargo, cuando los errores FTA son eliminados el rendimiento del conjunto disminuye con respecto al rendimiento en igualdad.

Por otro lado, el proceso en el que se utilizan los sensores en los escenarios de interoperabilidad tiene elevada influencia en el rendimiento del sistema conjunto, dado que éste aumenta o disminuye con respecto al sensor de reclutamiento en función del sensor de reconocimiento. Por ello no se obtiene el mismo rendimiento en dos sistemas diferentes cuando el sensor de reclutamiento del primero y de reconocimiento del segundo son iguales y, el sensor de reconocimiento del primero es igual al de reclutamiento del segundo. Este concepto se aprecia en las Figura 41 y 47 donde el sistema NXT-FPC (Figura 41) tiene unas tasas de error menores que las que posee el sistema FPC-NXT (Figura 47).

Por último, comentar que el rendimiento de un conjunto dependa del sensor utilizado para el reclutamiento es debido a los requisitos de calidad de las muestras de reclutamiento eran mas restrictivos que los requisitos de calidad de las muestras de reconocimiento, dado que como se comento en el apartado 3.3.1, con el fin de conseguir una muestra de reclutamiento con buena calidad se eliminaron de la base de datos las muestras de reclutamiento cuyo NFIQ era igual a 5, acción que no se realizó con las muestras de reconocimiento.

6. CONCLUSIONES

Tras obtener las medidas de rendimiento de los sistemas estudiados se ha podido comprobar cómo varía el rendimiento de dichos sistemas cuando durante el proceso de identificación de una persona los sensores utilizados son iguales, y cuando son diferentes, como queda explicado en el apartado de análisis de los resultados. Con ello se cumple el objetivo primordial del presente proyecto, realizar un análisis de interoperabilidad de diferentes tecnologías.

Tanto en el apartado de motivación como en el del marco socio-económico se mencionaron distintas aplicaciones en las que en la mayoría de los casos se utilizan sensores diferentes en el proceso de identificación de los usuarios, también se mencionó que este tipo de identificación se introducía con el fin de aumentar la seguridad de los sistemas de identificación tradicionales. Al realizar este proyecto buscando estudiar un problema real las conclusiones finales se dan en base a la situación que incluye en el análisis de los resultados los datos con errores FTA.

La principal cuestión que surgía era conocer si se puede colocar un sensor para el reconocimiento, diferente al utilizado en el reclutamiento, en general con peores prestaciones, con el fin de hacer menores los gastos invertidos en el sistema de identificación. Pues bien, esta cuestión depende de la seguridad que se requiera para el sistema de identificación, dado que, al comprobar que el rendimiento de los sensores disminuye si se utiliza un sensor de reconocimiento con peor rendimiento que el utilizado para el reclutamiento. Si la seguridad que se requiere no tiene por qué ser muy elevada, como puede ser el acceso a la máquina de café de una oficina, se podrá colocar un sensor de reconocimiento con peor rendimiento que el del reclutamiento. Sin embargo si el sistema de identificación se coloca en la entrada a un aérea restringida donde únicamente pueden acceder las personas autorizadas se necesitará una seguridad muy estricta, lo que provoca que sea recomendable colocar como sensor de reconocimiento el mismo sensor con el que se realizó el reclutamiento de las personas autorizadas.

También se puede dar el caso en el que el sensor que se colocó en un sistema que necesita elevada seguridad haya dejado de comercializarse, en este caso se debería colocar como sensor de reclutamiento uno cuyo rendimiento supere al anteriormente utilizado.

Según se observó en el apartado 3.3, las imágenes de los sensores NXT y UPK guardan mayor semejanza entre ellas que con las imágenes del sensor FPC, dado que el contraste de este último es inverso a los dos restantes. Una vez conocido el rendimiento de cada uno de los tres sensores, se observa como el comportamiento del sensor UPK se asemeja más al comportamiento del sensor NXT, a pesar de poseer una tecnología diferente, que al del sensor FPC, con quien comparte la misma tecnología. Por ello se afirma que en la interoperabilidad de los sensores tiene mayor influencia la semejanza de imágenes capturadas que la tecnología de los sensores utilizados.

6.1 Líneas futuras

Del mismo modo que ocurre con la mayoría de proyectos, el presente experimento podría ser ampliado en un proyecto futuro, principalmente en el concepto de la semejanza de las imágenes de dos sensores, NXT y UPK, y las diferencias de estas con las imágenes del tercero, FPC.

Dada esta diferencia como proyecto futuro se podría realizar un análisis muy parecido, consiguiendo unas imágenes de FPC que guardasen mayor semejanza con las de los sensores restantes. Este cambio podría conseguirse modificando el contraste en dichas imágenes haciendo que las huellas de las imágenes de FPC sean representadas con un tono gris sobre fondo blanco, lo que haría que se manejasen en los tres sensores imágenes muy parecidas.

De esta manera se podrían obtener nuevos rendimientos en los sistemas estudiados, y, probablemente los comportamientos de los tres sensores fuesen más semejantes que los obtenidos en el presente proyecto.

BIBLIOGRAFÍA

[1] ISO/IEC 19795-1:2006, Information technology - Biometric performance testing and reporting - Part 1: Principles and framework

[2] LOPD 15/1999 Ley Orgánica de Protección de Datos de Carácter Personal

[3] María Belén Fernández Saavedra, "Sistemas de identificación biométrica y su evaluación", Universidad Carlos III de Madrid.

[4] Mario Navalpotro Molina, "Estudio y análisis comparativo de las actuales técnicas de identificación biométrica", Universidad politécnica de Madrid, Junio 2014.

[5] Davide Maltoni, Dario Maio, Anil K. Jain, Salil Prabhakar: "Handbook of Fingerprint Recognition". New York, Springer, 2003

[6] Universidad nacional Autónoma de México, "Clasificación de los sistemas biométricos".

[7] Esteban Saavedra López, "Biometría y Patrones para la Identificación Humana".

[8] Raúl Sánchez Reillo, "Identificación Biométrica y su unión con las Tarjetas Inteligentes", Revista SIC, Apr 2000

[9] Umanick, "CUADERNOS DE BIOMETRÍA, HABLEMOS DE BIOMETRÍA", UMANICK LABS, S.L., 2012.

[10] Javier Ortega García, Fernando Alonso Fernández, Rafael Coomonte Belmonte, "Biometría y Seguridad", Cuadernos Cátedra ISDEFE. Universidad Politécnica de Madrid, May 2008.

[11] Umanick, "Hablemos de biometría: Ventajas y Desventajas", Jul 2013.

[12] Observatorio de la Seguridad de la Información de INTECO, "Estudio sobres las tecnologías biométricas aplicadas a la seguridad", Dic 2011.

[13] Mensaje publicado en: https://es.wikipedia.org/wiki/Huella_dactilar .

[14] Imagen recuperada de: http://curiosidades.batanga.com/sites/curiosidades.batanga.com/files/Esposible-nacer-sin-huellas-dactilares-1.jpg

[15] Imagen recuperada de: https://republicacientifica.files.wordpress.com/2012/07/huellas-digitales.jpg

[16] Barbazán Posse, Candela Casalderrey Carballal, Ana, "Huella digital"

[17] Mensaje publicado en: http://www.monografias.com/trabajos94/huellas-dactilares/huellas-dactilares.shtml#historiada

[18] Juan López García, "Algoritmo para la identificación de personas basado en huellas dactilares" Jul 2015.

[19] Imagen recuperada de: http://principiodeidentidad.blogspot.com.es/2008/01/biografa-de-juan-vucetich.html

[20] Enrique Vila-Matas (2010. 26 de Septiembre). Historia universal de la huella. El País. Edición Impresa y digital.

[21] Imagen recuperada de: http://thumbs.dreamstime.com/z/huella-digital-17361990.jpg

[22] Imagen recuperada de: http://mlm-s1-p.mlstatic.com/lector-de-huella-digitalpersona-4000b-con-sdk-modulo-nuevo-15416-MLM20103040899_052014-O.jpg

[23] Imagen recuperada de: http://www.monografias.com/trabajos82/biometria-y-voto-electronico/biometria-y-voto-electronico2.shtml

[24] Imagen recuperada de: http://www.biometricos.cl/equipos_biometria/images/fotos_docs/image4377.gif

[25] Imagen recuperada de: http://www.nist.gov/customcf/get_pdf.cfm?pub_id=51097

[26] Imagen recuperada de: 2009_Biometric System and Data Analysis.

[27] Imagen recuperada de: 2009_Biometric System and Data Analysis.

[28] Javier Galbally Herrero, "INTEROPERABILIDAD, USABILIDAD Y PRIVACIDAD EN SISTEMAS BIOMÉTRICOS MULTIMODALES"

[29] Mensaje publicado en http://www.informaticamoderna.com/Lect_huella.htm#defi

[30] Imagen recuperada de: http://tecelectronica.com.mx/promos/bit/bit0903huella_capac.gif.

[31] Mensaje publicado en: http://www.nist.gov/itl/iad/ig/nbis.cfm

[32] Mensaje publicado en: http://www.nist.gov/customcf/get_pdf.cfm?pub_id=51097

[33] Mensaje publicado en: https://msdn.microsoft.com/es-es/library/fx6bk1f4(v=VS.90).aspx

[34] Mensaje publicado en: https://es.wikipedia.org/wiki/Microsoft_Visual_Studio

[35] Mensaje publicado en: https://msdn.microsoft.com/es-es/library/Bb384488(v=VS.90).aspx

[36] Mensaje publicado en: http://es.mathworks.com/products/matlab/

[37] Carmen Sánchez Ávila. "Aplicaciones de la Biometría a la Seguridad". Centro de Domótica Integral (CEDINT), Universidad Politécnica de Madrid

ANEXO A: Planificación y presupuesto

Para este apartado se reserva un desglose de las tareas realizadas durante el presente Trabajo Fin de Grado, con el fin de facilitar el posterior cálculo sobre su coste.

A.1 Planificación

Dada la complejidad de este tipo de trabajos se ha optado por realizar un desglose de las diferentes fases del trabajo realizado.

Fase 1: Documentación inicial

1. Asistencia a una charla sobre biometría (4 horas)
2. Preparación de las herramientas de trabajo necesarias (4 horas)
3. Estudio previo de las plataformas a utilizar (10 horas)
4. Estudio del lenguaje de programación utilizado C# (20 horas)

Fase 2: Desarrollo de la aplicación en Visual Studio

1. Estudio de la plataforma Visual Studio y del entorno de desarrollo (20 horas)
2. Búsqueda de tutoriales y creación de aplicaciones sencillas (25 horas)
3. Comprensión de la herramienta NBIS (10 horas)
4. Desarrollo e implementación de la solución (70 horas)
5. Pruebas en la base de datos provisional, corrección y depuración del código (15 horas)

Fase 3: Desarrollo de la aplicación en Matlab

1. Estudio de la plataforma Matlab (3 horas)
2. Comprensión de la herramienta "Biosecure Tool" (6 horas)
3. Implementación de la solución (15 horas)
4. Pruebas provisionales, corrección y depuración del código (4 horas)

Fase 4: Pruebas con la base de datos real

1. Realización de los experimentos necesarios en Visual Studio(30 horas)
2. Obtención de las medidas de rendimiento en Matlab (15 horas)

Fase 5: Elaboración de la memoria

1. Redacción de la memoria (75 horas)
2. Corrección y maquetación (15 horas)

Tabla 7: Desglose de las tareas realizadas

FASES DEL TRABAJO REALIZADO	HORAS EMPLEADAS
Documentación inicial	38
Desarrollo de la aplicación en Visual Studio	140
Desarrollo de la aplicación en Matlab	28
Pruebas con la base de datos real	45
Elaboración de la memoria	90
TOTAL	**341**

A.2 Presupuesto del Trabajo Fin de Grado

A.2.1 Coste de materiales

Los materiales necesarios han sido:

- Un ordenador, con elevadas prestaciones de cara al procesamiento de imágenes, con el fin de obtener un funcionamiento correcto de la aplicación y reducir al máximo el tiempo empleado en la comparación de las imágenes.
- Una base de datos, en nuestro caso con un volumen de 50 usuarios.

Considerando un periodo de amortización para el ordenador de tres años, y teniendo en cuenta que la base de datos utilizada es el 11.6 % de la base de datos generada durante el periodo de prácticas de empresa, los costes de los materiales quedan como se expone en la Tabla 7. Además, se incluyen los gastos de licencias de software utilizados, para este proyecto únicamente ha sido necesaria la licencia del programa Matlab, ya que tanto la herramienta NBIS como "Biosecure Tool" son de dominio público, lo que hace que tengan un coste de licencia nulo.

Tabla 8: Coste de los materiales utilizados

CONCEPTO	PRECIO (€)
Ordenador de altas prestaciones	150
Base de datos utilizada	675
Licencia Matlab	59
TOTAL	**884**

A.2.2 Coste de personal

A los gastos de material hay que añadir los gastos de personal, dado que para la realización de este trabajo ha sido necesaria la presencia, a tiempo parcial de un director de proyecto, un jefe de proyecto y la presencia, a tiempo completo, de un ingeniero. Datos reflejados en la Tabla 9

Tabla 9: Coste de personal

OCUPACIÓN	HORAS	PRECIO/HORA	IMPORTE (€)
Director de proyecto	5	90	450
Jefe de proyecto	25	60	1.500
Ingeniero	311	30	9.330
TOTAL	**341**		**11.280**

A.2.3 Coste total

Tabla 10: Coste total del proyecto

CONCEPTO	PRECIO(€)
Coste de materiales	884
Coste de personal	11.280
Costes indirectos (15%)	1.692
Subtotal	13.856
IVA (21%)	2.909,76
TOTAL	16.765,76

El coste total del proyecto es de DIECISEISMIL SETECIENTOS SESENTA Y CINCO EUROS CON SETENTA Y SEIS CÉNTIMOS.